DoD Manual 5200.02

Procedures for the DoD Personnel Security Program (PSP)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective: **Change 1 Effective:**	April 3, 2017 October 29, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	DoD 5200.2-R, "Personnel Security Program," January 1987 Under Secretary of Defense for Intelligence Memorandum, "Minimum Requirements for Interim Eligibility to Access Secret and Confidential Information," January 17, 2014
Approved by:	Todd R. Lowery, Performing the Duties of the Under Secretary of Defense for Intelligence
Change 1 (Administrative) Approved by:	Christopher R. Choate, Chief, Directives Division

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and DoD Instruction (DoDI) 5200.02, the issuance implements policy, assigns responsibilities, and provides procedures for the DoD PSP. This issuance:

- Assigns responsibilities and prescribes procedures for investigations of individuals seeking to hold national security positions or perform national security duties who are required to complete Standard Form (SF) 86, "Questionnaire for National Security Positions," for personnel security investigations (PSIs).
- Sets procedures for DoD PSP national security eligibility for access determinations; personnel security actions; continuous evaluation (CE); and security education requirements for employees seeking eligibility for access to classified information or to hold a sensitive position (referred to in this manual as "national security eligibility").
- Prescribes procedures for administrative due process for employees. Administrative due process for **contractor personnel** is governed by DoDD 5220.6.

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the National Guard Bureau, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. INFORMATION COLLECTIONS.

a. The PSP policy and procedures assessments, referred to in Paragraph 2.2.d of this manual, does not require licensing with a report control symbol in accordance with Paragraph 1b(9) of Section 3 to Volume 1 of DoD Manual 8910.01.

b. Annual DoD PSI Projections Report, referred to in Paragraph 2.10.c of this manual, has been assigned report control symbol DD-INT(A)2641 in accordance with the procedures in Volume 1 of DoD Manual 8910.01.

c. The Inspector General reports, referred to in Paragraph 2.10.q of this manual, do not require licensing with a report control symbol in accordance with Paragraph 1b(6) of Section 3 to Volume 1 of DoD Manual 8910.01.

d. The annual limited access authorization (LAA) Summary Report, referred to in Paragraph 6.1.c. of this manual, has been assigned report control symbol DD-INT(A)2642 in accordance with the procedures in Volume 1 of DoD Manual 8910.01.

e. The Bond Amendment Waiver Report, referred to in Paragraph 7B.3.e. of this manual, does not require licensing with a report control symbol in accordance with Paragraph 1b(16) of Section 3 to Volume 1 of DoD Manual 8910.01.

1.3. SUMMARY OF CHANGE 1. This administrative change updates:

a. The title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92.

b. Additional organizational changes reflecting direction in statute or Secretary and Deputy Secretary of Defense direction.

c. Administrative changes in accordance with current standards of the Office of the Chief Management Officer of the Department of Defense

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S):

a. Serves as the DoD Senior Security Official.

b. Develops policy, guidance, and oversight for the DoD Personnel Security Program (PSP), in accordance with DoDD 5143.01, in that capacity reviews and approves DoD Components' policy and procedures governing civilian, military, and contractor personnel PSPs within the DoD.

c. Ensures that the DoD PSP is consistent, cost effective, efficient, and balances the rights of individuals with the interests of national security.

d. Coordinates with the General Counsel of the Department of Defense (GC DoD) to ensure legal sufficiency of DoD personnel security policy and procedures, in accordance with DoDI 5145.03.

e. Oversees DoD national security investigations, adjudications, and access determinations pursuant to Executive Order (E.O.) 12968 and national security adjudicative guidelines in the August 30, 2006 Under Secretary of Defense for Intelligence (USD(I)) Memorandum.

f. Issues and interprets all policies governing the Joint Personnel Adjudication System (JPAS), as defined in the Glossary.

g. Oversees the implementation of PSP policy pertaining to sensitive compartmented information (SCI) pursuant to Chapter 3 of Title 5, United States Code (U.S.C.), and Intelligence Community Directive Number 704.

h. Develops and oversees administration of that portion of the DoD PSP pertaining to DoD Special Access Programs (SAPs) in accordance with DoDD 5205.07.

i. Oversees integration of PSP requirements in other DoD issuances.

j. Ensures DoD Components integrate security education and awareness into their PSPs.

k. Requires DoD Components to adequately resource their programs for military, civilian, and contractor personnel investigations and meet established personnel security policies and procedures.

l. Coordinates with investigative service providers (ISPs) on background investigation quality issues in accordance with national policy and inter-agency agreements.

m. Monitors DoD compliance with Section 3341 of Title 50, U.S.C. investigative and adjudicative timelines.

n. Approves adoption of DoD enterprise-wide personnel security systems of record.

o. Issues and interprets policy for the Adjudicator Professional Certification (APC) program.

p. Reviews and makes determinations on DoD Component requests for waivers to personnel security policy.

q. Issues policy, assigns responsibilities, and prescribes procedures for CE within the DoD Personnel Security Program, in accordance with E.O. 12968.

2.2. DIRECTOR, DEFENSE INTELLIGENCE (INTELLIGENCE AND SECURITY) (DDI&I&S)). Under the authority, direction, and control of the USD(I&S), the DDI(I&S):

a. Oversees DoD personnel security policy matters.

b. Provides staff assistance to the DoD Components in resolving day-to-day personnel security policy and operating problems.

c. Provides personnel security policy guidance and interpretation to the DoD Components.

d. Assesses the DoD Components for implementation and compliance with DoD PSP policy and procedures.

e. Approves, coordinates, and oversees all DoD personnel security research initiatives and activities, excluding research efforts relating to individual DoD Components.

2.3. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I&S), in addition to the responsibilities in Paragraph 2.10 and in accordance with DoDD 5105.42, the Director, DSS:

a. Reports to USD(I&S) Security Policy and Oversight Division by May 15 the annual contractor personnel PSI workload projections for the National Industrial Security Program (NISP), to include the number and type of clearances required and funding requirements in accordance with DoDI 5220.22.

b. Budgets, funds, and submits background investigation requests for contractor personnel who require access to classified information under the NISP.

c. Processes, reviews, and grants interim personnel security eligibility for contractor personnel under the NISP where DoD serves as the Cognizant Security Agency (CSA) in accordance with DoDI 5220.22.

d. Determines, after consultation with the GC DoD, when action should be taken in the interests of national security to suspend a contractor personnel clearance eligibility in accordance with the provisions of Volume 2 of DoDM 5220.22 and the May 13, 2009 USD(I) Memorandum.

e. Establishes and administers education, training, and certification programs for the personnel security discipline and related systems (e.g., the Security Professional Education Development Program (SPēD)) in accordance with DoDI 3305.13 and JPAS.

f. Maintains certification records and related documentation in accordance with DoDI 3305.13 and DoD 3305.13-M.

g. Confirms that the applicable government contracting activity has a valid need before approving extensions of interim eligibility beyond 1 year.

2.4. GC DOD. The GC DoD, in consultation with the USD(I&S) and pursuant to DoDI 5145.03, establishes guidance, provides legal advice, and exercises legal oversight of the DoD PSP to ensure fair, timely, and consistent treatment of individuals and to verify that the rights of individuals are being protected in accordance with the Constitution, laws of the United States, E.O.s, and DoD policy.

2.5. DIRECTOR, DEFENSE OFFICE OF HEARINGS AND APPEALS (DOHA). Under the authority, direction, and control of the GC DoD, the Director, DOHA, conducts hearings and appeals in accordance with this manual and DoDD 5220.6 as applicable.

2.6. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) provides applicable position designation guidance, integrating and complementing existing regulations (e.g., information assurance, information technology, Counterintelligence (CI)) to the DoD Components as established in the May 10, 2011 USD(P&R) Memorandum.

2.7. DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY (DODHRA). Under the authority, direction, and control of the USD(P&R), the Director, DoDHRA, through the Director, Defense Manpower Data Center:

a. Plans, programs, executes, updates, and maintains information technology systems to support the DoD PSP as well as future initiatives and applications approved by the USD(I&S) (e.g., automated clean case screening and automated records checks).

b. Coordinates with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), DoD Consolidated Adjudication Facility (CAF), DoD Components, and the Office of the Chief Management Officer of the Department of Defense (CMO) to develop, coordinate, and publish procedures and processes on the management and accessibility of data in JPAS.

c. Sustains personnel security databases, applications, and collateral operations in accordance with the February 2, 2010 Memorandum of Agreement.

d. Provides personnel security data to the OUSD(I&S) and to DSS as requested by OUSD(I&S).

e. Provides analysis, research, and development support through the Defense Personnel and Security Research Center to OUSD(I&S), to advance DoD personnel security policy, programs, and DoD and Executive Branch reform efforts.

2.8. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). In coordination with the Director, DSS, the USD(AT&L) establishes policies and procedures to ensure applicable personnel security requirements for classified access in contracts are enforced.

2.9. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the CMO, and in addition to the responsibilities in Paragraph 2.10, the Director, WHS:

a. Conducts national security eligibility adjudications for the Department of the Army, Department of the Navy, Department of the Air Force, Joint Chiefs of Staff, contractor employees, and DoD agencies in accordance with the October 20, 2010 Deputy Secretary of Defense Memorandum, and for personnel outside the Executive Branch and for certain non-DoD Agencies pursuant to agreements.

b. Establishes policy and procedures, in conjunction with OUSD(I&S), for DoD Consolidated Adjudications Facility (DoD CAF operations).

c. Exercises certain head of the IC element authorities to determine Sensitive Compartmented Information (SCI) eligibility in accordance with the October 22, 2012 Director of National Intelligence (DNI) Memorandum.

d. Establishes a quality assurance program that:

(1) Determines the completeness of national security investigations and adjudicative rationales in accordance with the November 8, 2009 and August 31, 2010 USD(I) Memorandums.

(2) Evaluates incomplete national security investigations in accordance with the July 13, 2010 and March 10, 2010 USD(I) Memorandums.

2.10. DOD COMPONENT HEADS. The DoD Component heads:

a. Appoint a senior security official to be responsible for direction, overall management, functioning, and administration of the Component's PSP.

b. Provide a point of contact (POC) for PSI workload projections to OUSD(I&S).

c. Provide annual PSI workload projections to OUSD(I&S) no later than May 15. PSI projections should be within 5 percent of actual submissions.

d. Commit resources to satisfy projected PSP, PSI, and reinvestigation requirements to include contractor personnel PSIs when eligibility is required for positions of trust without access to classified information.

e. Validate and ensure prompt payment of ISP bills for all investigations ordered.

f. Ensure applicable personnel security requirements are included in all contracts, agreements, memorandums of understanding, and other similar documents.

g. Establish and maintain an ongoing self-inspection program to annually evaluate and assess the effectiveness and efficiency of the Component's implementation of the DoD PSP.

h. Direct commanders and activity heads to designate, in writing, an activity personnel security manager and, as appropriate, activity assistant security managers, who are given the authority to assist in program implementation, maintenance, and local oversight to ensure personnel adhere to program requirements. The activity personnel security manager will have direct access organizationally to activity leadership and will be organizationally aligned to oversee prompt and appropriate attention to PSP requirements.

i. Provide guidance, direction, and oversight necessary to ensure an appropriate training program addressing personnel security (e.g., SPēD) is administered effectively and in accordance with DoDI 3305.13 and DoD 3305.13-M.

j. Report information of a CI or security concern to the appropriate CI, law enforcement, or security authority in accordance with law and policy. Develop, distribute, and oversee procedures to meet standard reporting requirements for issues of security concern pertaining to subjects of national security eligibility determinations in accordance with Section 11 of this manual.

k. Establish a program for employees with access to classified information to:

(1) Educate employees about individual responsibilities under the PSP.

(2) Inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

l. Provide security, CI, and country awareness briefings, including applicable geographic Combatant Command force protection briefings, to individuals before foreign travel and conduct post-travel debriefings in accordance with DoDD 5240.06, DoDI 5200.39, and Volume 1 of DoDI O-2000.16.

m. Ensure that results of investigations are delivered to the DoD CAF or appropriate DoD IC central adjudication facilities for adjudication regardless of the source of the original request

when requesting background investigations or reinvestigations for national security eligibility determinations.

n. Actively participate in the CE program as outlined in Section 11 of this manual.

o. Ensure personnel are trained on their security responsibilities in accordance with national security adjudicative guidelines in the August 30, 2006 USD(I) Memorandum, E.O. 13526, and the November 12, 2012 Presidential Memorandum and establish procedures to brief individuals at least annually.

p. Develop formal procedures to report misconduct, violations, or adverse information by contractor personnel to the appropriate adjudication facility.

q. Ensure inspector general investigations into misconduct by contractor personnel are recorded in the Defense Central Index of Investigations in accordance with DoDI 5505.07 and DoDI 5505.16 and are reported to DSS and the appropriate adjudication facility.

r. Submit and resource investigation requests for contractor personnel outside the NISP (i.e., investigations required for other than access to classified information).

s. Create and maintain records for contractor personnel investigations outside the NISP in the appropriate system of record.

t. Record access determinations and indoctrinations into the approved system of record and record access debriefings and separations as soon as individuals separate or terminate affiliation with the access granting authority.

u. Ensure personnel data in JPAS are valid, accurate, and current. Institute procedures to update data on a daily basis.

v. Ensure all Component actions support the opportunity for appeal and that actions required to process appeals are performed in accordance with the procedures in this manual.

w. Ensure requests for periodic reinvestigations are initiated in a timely manner, as described in Paragraph 3.6. of this manual.

x. Ensure contracts for contractor personnel in support of adjudications include requirements specified in Paragraph 4.7.b.

2.11. HEADS OF DOD IC ELEMENTS. In addition to the responsibilities in Paragraph 2.10, the heads of DoD IC elements will investigate, adjudicate, and grant eligibility for access to SCI and other controlled access program information pursuant to Title 5, U.S.C., Intelligence Community Directive 704, and Intelligence Community Policy Guidance Numbers 704.1, 704.2, 704.3, 704.4, and 704.5.

2.12. SECRETARY OF THE AIR FORCE. In addition to the responsibilities in Paragraph 2.10, the Secretary of the Air Force:

a. Serves as the single POC to provide information technology funding, hosting, and technical support for the Central Adjudication Security Personnel Repository or successor system to support the DoD's PSI billing responsibilities for military, civilian, and contractor personnel investigations, in accordance with the January 15, 2009 Deputy Secretary of Defense Memorandum and the August 6, 2009 Memorandum of Agreement between OUSD(I&S) and the Air Force.

b. Serves as the POC for military, civilian, and contractor personnel investigations to receive, manage, report on, monitor, evaluate, and resolve DoD bills for national security investigations from the U.S. Office of Personnel Management (OPM), in accordance with the August 6, 2009 Memorandum of Agreement between OUSD(I&S) and the Air Force. The POC:

(1) Provides copies of billing data to OUSD(I&S) and Defense Personnel Security and Research Center as needed.

(2) Notifies OUSD(I&S) of any unresolved billing issues.

(3) Conducts all financial transactions with OPM in accordance with Section 305, Chapter 3 of Volume 4 of DoD 7000.14-R.

SECTION 3: NATIONAL SECURITY INVESTIGATIONS

3.1. GENERAL. Military, civilian, contractor, consultant, and other affiliated personnel assigned to national security positions or required to perform national security duties will be subject to investigation to determine whether they are and will remain reliable, trustworthy, of good conduct and character, and loyal to the United States and whether granting or continuing national security eligibility is clearly consistent with the national interest.

a. Civilian position sensitivity will not be downgraded to facilitate recruitment or retention of personnel or to accommodate adverse security determinations.

b. Investigative requests will not be submitted for eligibility higher than what has been designated for the position or required for the duty to be performed.

c. Non-U.S. citizens who will require eligibility for access to classified information must follow the LAA procedures in Section 6 of this manual. The number of LAA requests must be minimized.

3.2. FEDERAL INVESTIGATIVE STANDARDS (FIS).

a. The OPM Federal Investigative Notice 97-02 provides a summary of the FIS and the scope of the investigations used to grant national security eligibility. Additional requirements that exceed the FIS are not authorized.

b. The FIS, established by the December 13, 2008 DNI and OPM Memorandum, are being deployed in phases. The standards apply to investigations that determine eligibility for access to classified information, to hold a national security position, for physical and logical access, and for suitability for government employment.

3.3. INVESTIGATIVE REQUIREMENTS.

a. Occupants of national security positions and those performing national security duties for any DoD Component are subject to investigation unless they meet the reciprocity standards in Section 3. Civilian employee investigative requirements for competitive and excepted service are the same.

b. Authorized investigations are:

(1) Single Scope Background Investigation (SSBI) or its Equivalent Under the FIS. SSBIs are conducted to meet investigation requirements established by DoDD 5105.42 for those seeking to hold special-sensitive or critical-sensitive positions, and those requiring eligibility for access to Top Secret (TS), SCI, and Department of Energy (DOE) "Q" level information.

(2) Access National Agency Check and Inquiries (ANACI) or its Equivalent Under the FIS. The ANACI is the required initial minimum investigative requirement for federal civilian

employees who require access to Secret, Confidential, or DOE "L" level classified information or eligibility to hold non-critical sensitive positions.

(3) National Agency Check with Law and Credit (NACLC) or its Equivalent Under the FIS. Except as required by Paragraph 3.3.b(2), the NACLC is the required minimum investigation for:

(a) Contractor personnel for eligibility for access at the Confidential, Secret, and DOE "L" levels.

(b) Individuals seeking entry into the Military Departments (active duty, guard, or reserve) in accordance with the January 8, 2004 Deputy Under Secretary of Defense Memorandum.

(c) Service members requiring eligibility for access to Secret, Confidential, and DOE "L" levels.

(d) Individuals other than federal civilian employees requiring eligibility to occupy non-critical sensitive positions such as a consultant.

(e) Federal employees, contractor personnel, and Service members for continued access to Confidential or Secret information. Reinvestigations are discussed in Paragraph 3.6.

c. Investigative requirements for other populations are outlined in Section 4 of this manual.

d. A SSBI, ANACI, NACLC, or an equivalent investigation completed within the past 5 years may be used to meet investigative requirements if the previous investigation was favorably adjudicated.

3.4. POLYGRAPH. The polygraph may be used as a personnel security screening measure in accordance with DoDD 5210.48 and as stated in Paragraph 4.10.

3.5. POST-ADJUDICATIVE INQUIRIES. Post-adjudicative inquiries may be conducted by adjudication facility personnel or an approved ISP, as appropriate, to resolve any issues pertinent to the guidelines discussed in national security adjudicative guidelines in the August 30, 2006 USD(I) Memorandum with respect to an individual's national security eligibility. CE and reporting requirements are addressed in Section 8 of this issuance.

3.6. REINVESTIGATIONS. In accordance with the FIS, reinvestigations may be performed at any time after national security eligibility has been granted. Additionally, DoD employees in national security positions and contractor personnel performing national security duties will be subject to periodic reinvestigation (PR) on a recurring basis as described in this section. Submission of out-of-cycle reinvestigations must be justified before approval of the submission.

a. PR requests will be submitted no earlier than 3 months before the respective anniversary date of the close date of the last investigation.

b. Military and civilian personnel for whom periodic investigative requests are initiated must have at least 12 months remaining in service or employment.

c. Every effort should be made to ensure PRs are conducted within the prescribed timeframe so as not to undermine the ability of the DoD to accomplish its mission.

(1) National security eligibility will not be administratively downgraded nor access suspended based solely on the fact that a reinvestigation was not completed within the specific timeframe as long as the required reinvestigation was requested within the specific timeframe. Failure or refusal to complete forms and requests for reinvestigations on a timely basis can be grounds for termination of eligibility and will be reported to the appropriate adjudicative facility. Commanders and supervisors, in coordination with the security professional, will enforce reinvestigation requirements.

(2) National security eligibility will not be terminated for individuals who are unavailable to submit the required reinvestigation due to extended operational deployments, illness, or like situations. DoD Components will make every effort to ensure the requisite background investigation is submitted before deployment or when the individual is otherwise unavailable for a prolonged period. Individuals must submit the reinvestigation promptly upon return to work or duty status.

d. A national security eligibility determination is deemed current if the reinvestigation is submitted to the investigation service provider within 5 years of the previous investigation close date. Personnel assigned to a North Atlantic Treaty Organization (NATO) staff positions may submit a reinvestigation request up to 1 year in advance of the required timeframe in accordance with DoDD 5100.55.

(1) Noncritical-sensitive or Equivalent Positions. The NACLC is the reinvestigation required for military, civilian, and contractor personnel requiring continuing eligibility for access to classified information no higher than Secret and for those civilian personnel occupying noncritical-sensitive positions. The reinvestigation will be initiated no later than 5 years from the close of the previous investigation.

(2) Special-sensitive and Critical-sensitive or Equivalent Positions. Each DoD military and civilian employee occupying a special-sensitive or critical-sensitive position and each contractor personnel requiring continuing national security eligibility at an equivalent level will undergo a reinvestigation initiated on a 5-year recurring basis. There are two types of reinvestigations for the SSBI. Security professionals should use the phased periodic reinvestigation disqualification table to determine the appropriate PR to request to conserve resources.

(a) Single Scope Background Investigation – Periodic Reinvestigation (SSBI-PR). The SSBI-PR must be requested if the subject discloses or the requestor is otherwise aware of information listed in the PPR disqualification table.

(b) Phased Periodic Reinvestigation (PPR). The PPR may be requested if the subject does not disclose anything of a security concern as part of the background information furnished for investigation. Select questions from the SF 86 constitute the criteria for determining when an SSBI-PR may be submitted as a PPR. Submit reinvestigations as PPRs unless a positive response is annotated for the items listed in the Table:

Table 1. PPR Disqualification

Citizenship	Subject is not a U.S. citizen, or has renounced or otherwise lost U.S. citizenship since the last investigation.
Dual Citizenship	Subject is a dual citizen or has obtained dual citizenship since the last investigation.
Foreign Activities	Subject has been employed by or acted as a consultant for any foreign government, firm, or agency; has engaged in any contact with a foreign government or its establishments or representatives on other than official U.S. Government business; or holds or has been issued a foreign passport.
Medical Record	Since the last investigation, subject has undergone mental health treatment that is reportable under Section 21 of the SF-86.
Police Record	Subject has been charged with or convicted of any criminal offenses (excluding traffic violations that do not involve alcohol or drugs, resulting in fines less than $300) since the last investigation.
Use of Alcohol	Subject has abused alcohol or has received any alcohol-related treatment or counseling since the last investigation.
Unauthorized Use of Illegal Drugs and Drug Activity	Subject has used any drugs illegally since the last investigation.
Financial Records	Subject provided positive response to questions regarding bankruptcy; gambling; failing to file or pay taxes; violation of government credit or travel card; seeking credit counseling; having financial issues involving court, Internal Revenue Service, or similar enforcement; or financial issues involving routine accounts.
Investigation Record	Subject has had an access authorization denied, suspended, or revoked, or has been barred from federal employment since the last investigation.
Association Record	Subject has associated with any individuals or groups dedicated to the violent overthrow of the U.S. Government or has acted to do so.

SECTION 4: SPECIFIC INVESTIGATIVE REQUIREMENTS BY POPULATION

4.1. CIVILIAN PERSONNEL.

a. Civilian Positions and Sensitivity Levels. Position designations are necessary to determine the requisite type of investigation. Consistent with the requirements of Part 732 of Title 5, U.S.C., DoD Components will designate civilian positions (competitive service, excepted service, Senior Executive Service, or other civilian positions, as prescribed in E.O. 10450 that require the occupant to perform national security duties as an employee of the federal Government with a sensitivity level in accordance with the May 10, 2011 USD(P&R) Memorandum and, as applicable, OPM guidance). Civilian position sensitivity will not be downgraded solely to facilitate recruitment or retention of personnel or to accommodate adverse security determinations. There are three levels of sensitivity pursuant to Part 732 of Title 5, U.S.C. that pertain to civilian personnel in national security positions:

(1) Special-sensitive. A special-sensitive civilian national security position is one with potential for inestimable damage to the national security or for inestimable adverse impact to the efficiency of the Department or the Military Departments. This includes:

(a) Positions requiring eligibility for access to SCI.

(b) Positions requiring eligibility for access to unique or uniquely productive intelligence-related special-sensitive information or involvement in SAPs.

(c) Any other civilian position the DoD Component head determines to be at a higher level than critical-sensitive due to special requirements that complement E.O. 12968 and E.O. 10450.

(2) Critical-sensitive. Any civilian national security position that has the potential to cause exceptionally grave damage to the national security including, but not limited to:

(a) Positions requiring eligibility for access to TS or DOE "Q" level classified information.

(b) Positions involving development or approval of war plans, major or special operations of war, or critical and extremely important items of war.

(c) National security policy-making or policy-determining positions, the duties of which have the potential to cause exceptionally grave damage to the national security.

(d) Positions involving investigative duties, including handling of CI investigations or background investigations, the nature of which has the potential to cause exceptionally grave damage to the national security.

(e) Positions related to the adjudication, recommendation of adjudicative determinations, or granting of national security eligibility.

(f) Positions involving duty on personnel security boards.

(g) Positions concerned with development or approval of plans, policies, or programs that affect overall DoD or DoD Component operations.

(h) Positions related to the conduct of CI activities.

(i) Senior management positions in key programs, the compromise of which could result in grave damage to the national security.

(j) Positions having direct involvement with diplomatic relations and negotiations.

(k) Positions involving independent responsibility for planning or approving continuity of government operations.

(l) Positions involving major and immediate responsibility for, and the ability to act independently without detection to compromise or exploit, the protection, control, and safety of the nation's borders and ports or immigration or customs control or policies, where there is a potential to cause exceptionally grave damage to the national security.

(m) Positions involving major and immediate responsibility for and the ability to act independently without detection to compromise or exploit the design, installation, operation, or maintenance of critical infrastructure systems or programs.

(n) Positions in which the occupant has the ability to independently damage public health and safety with devastating results.

(o) Positions in which the occupant has the ability to independently compromise or exploit biological select agents or toxins, chemical agents, nuclear materials, or other hazardous materials.

(p) Positions in which the occupant has the ability to independently compromise or exploit the nation's nuclear or chemical weapons designs or systems.

(q) Positions in which the occupant obligates, expends, collects, or controls revenue, funds, or items with monetary value in excess of 50 million dollars, or procures or secures funding for goods or services with monetary value in excess of 50 million dollars annually, with the potential for exceptionally grave damage to the national security.

(r) Positions in which the occupant has unlimited access to and control over unclassified information, which may include private, proprietary, or other controlled unclassified information, but only where the unauthorized disclosure of that information could cause exceptionally grave damage to the national security.

(s) Positions in which the occupant has direct, unrestricted control over supplies of arms, ammunition, or explosives or control over any weapons of mass destruction.

(t) Positions in which the occupant has unlimited access to or control of access to designated restricted areas or restricted facilities that maintain national security information classified at the TS or "Q" level.

(u) Positions working with significant life-critical or mission-critical systems, such that compromise or exploitation of those systems would cause exceptionally grave damage to essential government operations or national infrastructure.

(v) Positions in which the occupant conducts internal or external investigation, inquiries, or audits related to the functions described in Paragraphs 4.1.a(2)(a) through 4.1.a(2)(u), where the occupant's neglect, action, or inaction could cause exceptionally grave damage to the national security.

(w) Positions so designated by the DoD Component head.

(3) Noncritical-sensitive. Any civilian national security position that has the potential to cause significant or serious damage to the national security. This may include civilian national security positions:

(a) Requiring eligibility for access to Confidential, Secret, or DOE "L" level information.

(b) Not requiring eligibility for access to classified information, but having the potential to cause significant or serious damage to the national security.

(c) With access to automated systems that contain military active duty, guard, or reservists' personally identifiable information or information pertaining to Service members that is otherwise protected from disclosure by DoD 5400.11-R where such access has the potential to cause serious damage to the national security.

(d) Designated by the DoD Component head.

b. Investigative Requirements and Civilian Positions.

(1) Special-sensitive and Critical-sensitive. Civilian personnel in special-sensitive and critical-sensitive positions require a favorably adjudicated SSBI or its equivalent.

(2) Noncritical-sensitive. Civilian personnel in noncritical-sensitive positions require a favorably adjudicated ANACI or its equivalent. A NACLC or its equivalent may be used for appointment provided an ANACI has been requested from an authorized ISP and there is no more than 24 months break in service.

4.2. MILITARY PERSONNEL.

a. The appointment, enlistment, and induction of each member of the Military Departments or their Reserve Components will be based on a favorably adjudicated PSI.

b. The NACLC, or its equivalent, is the minimum investigation required for entry into the Military Departments.

c. The NACLC, or its equivalent, will be conducted upon re-entry to any Military Department component when there has been a break in service longer than 24 months.

4.3. CONTRACTORS. PSI requirements for contractor personnel requiring national security eligibility are addressed in DoD 5220.22-M.

4.4. CONSULTANTS AND GRANTEES OF A DOD COMPONENT.

a. A consultant or grantee who is directly engaged by a DoD Component (as opposed to an employee of a contractor) and requires national security eligibility only at the Component's activity or in connection with authorized visits does not fall under the NISP. For purposes of national security adjudicative guidelines in the August 30, 2006 USD(I) Memorandum and this manual, investigations for such personnel will proceed in the same manner as for DoD Component employees. The consultant or grantee will be issued national security eligibility in accordance with the guidance in this manual.

b. Investigations required to support the consultant's or grantee's national security eligibility will be conducted by the designated ISP and adjudicated by a DoD adjudication facility.

c. When compelling reasons exist, non-U.S. citizens functioning as consultants or grantees to the DoD Components may be considered for LAA as specified in Section 3 of this manual.

4.5. NON-U.S. CITIZENS EMPLOYED OVERSEAS IN SUPPORT OF NATIONAL SECURITY POSITIONS.

a. A non-U.S. citizen employed by the DoD Components overseas, who provides support to national security positions and who does not require access to classified information, will be subject to the following record checks initiated (before employment) by the DoD Components. International, bi-lateral, or subsidiary agreements governing locally hired employees may require additional investigation. The minimum required checks are:

(1) Host government law enforcement and security agency checks at the city, State (province), and national level whenever permissible by the laws of the host government and when practical, considering CI responsibilities in accordance with DoDD 5240.02.

(2) DoD-approved automated records checks.

(3) Federal Bureau of Investigation (FBI) records (where information exists indicating residence by the non-U.S. citizen in the United States for 1 year or more since age 18).

b. The DoD Components assume responsibility for permitting access to DoD systems, unclassified information, material, and areas when an investigation conducted by the host country does not meet the investigative standards of this manual.

c. The DoD Components will allow access to unclassified information by a non-U.S. citizen only in accordance with applicable disclosure policies and when such access cannot cause significant or serious damage to U.S. national security.

d. The DoD Components may choose to include additional checks as appropriate.

4.6. TEMPORARY EMPLOYEES. Unless approved as a waiver by the DoD Component senior security official or the head of an IC element (in the case of SCI), temporary, intermittent, summer hires, and seasonal employees (not to exceed 180 days) will not be assigned to special-sensitive or critical-sensitive positions. Any temporary, intermittent, summer hire, or seasonal employee who is granted national security eligibility must be 18 years of age or older on or before national security eligibility is granted. Copies of all waivers granted will be provided to the DDI(I&S).

4.7. WOUNDED WARRIOR SECURITY AND INTELLIGENCE INTERNSHIP PROGRAM (WWSIIP). PSIs in support of designated wounded Service members may be submitted and processed regardless of the time remaining in service.

a. Category 2 wounded, ill, or injured Service members who expect to be separated with a medical disability rating of 30 percent or greater may submit investigative requests for TS with SCI access eligibility before medical separation as long as they are serving in or have been nominated for a wounded warrior internship program.

b. The investigations will be funded by the DoD office offering the internship. If the office offering the internship does not have funds available, the owning Military Department may choose to fund the investigation.

c. Investigations submitted in support of WWSIIP should:

(1) **Not** request priority service.

(2) Include the extra coverage code "WW" in Block B of the "Agency Use Only" section of the SF 86. This will expedite scheduling and completion of investigations submitted in support of the WWSIIP.

(3) Notify OPM via e-mail to operationwarfighter@opm.gov. Include the subject's full name, the electronic application (e-application) request identification number, and the DoD POC should OPM need additional information.

4.8. RETIRED GENERAL OR FLAG OFFICER (GO/FO) OR CIVILIAN EQUIVALENT.

a. An active duty GO/FO or civilian equivalent may determine that there are compelling reasons to grant a retired GO/FO or civilian equivalent access to classified information in connection with a specific DoD program or mission. In these instances, an active duty GO/FO or civilian equivalent may provide access to classified information for a period not to exceed 1 year. Further, in these instances, the investigative requirements of this manual may be waived. The access will be limited to classified information at a level commensurate with the security eligibility held at the time of retirement, or within 24 months before retirement, but excludes access to SAPs. Access to SAPs requires compliance with access eligibility review as determined by the SAP Central Office with cognizant or oversight authority.

b. Requests for SCI or SAP access will be processed in accordance with this manual, DNI policy, and DoDD 5205.07, as applicable.

c. The GO/FO or civilian equivalent approving the access to classified information will provide the appropriate adjudication facility a written record of the following data for retention in the DoD adjudicative system of record for 2 years after access is granted:

(1) The name and social security number of the former employee granted access.

(2) The date and level of access authorized.

(3) Compelling reason to grant the access and the benefit to the DoD mission or event.

(4) Identity of the approving authority.

d. The classified materials involved will not be removed from the confines of a government installation or other area approved for storage of DoD classified information.

4.9. RED CROSS AND UNITED SERVICE ORGANIZATION (USO) PERSONNEL.

a. Red Cross and USO employees will be accepted for assignment or for continued assignment with Military Departments overseas or for national security eligibility provided acceptance is consistent with the national interest and DoD personnel security policy.

b. U.S. citizen employees in national security positions will undergo an NACLC or its equivalent investigation before being nominated for assignment with the Military Departments overseas.

c. Non-U.S. citizen employees will undergo an investigation as outlined in Paragraph 4.5.

d. A completed SF 86 will be forwarded to the ISP for the initiation of the investigation, if applicable.

e. The results of the investigation will be forwarded to the DoD CAF for an eligibility determination of the employee. The DoD CAF records these determinations in the DoD adjudication system of record.

f. Whenever information of an adverse nature is received indicating that an employee's assignment or continued assignment with the Military Departments overseas may not be consistent with the national interest, the information will be forwarded to the DoD CAF to initiate or expand the investigation.

g. Due process provisions in DoDD 5220.6 apply to Red Cross and USO personnel.

h. The DoD CAF will serve as the contact for the Red Cross and USO in all matters pertaining to the procedures stated, while the DOHA will provide all due process.

4.10. PERSONS OUTSIDE THE EXECUTIVE BRANCH. National security eligibility held by persons outside the Executive Branch will be accomplished in accordance with Chapter 15 of Title 50, U.S.C. The investigative requirement will be the same as for persons inside the Executive Branch at the appropriate level of national security eligibility, except as indicated:

a. Members of the U.S. Senate and House of Representatives do not require national security eligibility for access to DoD classified information. They may be granted access to DoD classified information that relates to matters under the jurisdiction of the respective committees to which they are assigned and is needed to perform their duties in connection with such assignments.

b. Members of the U.S. Supreme Court, the federal judiciary, and the Supreme Courts of the individual States do not require national security eligibility. They may be granted access to DoD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

c. State governors do not require national security eligibility. They may be granted access to specifically designated classified information on a need-to-know basis, which is contingent upon affirmation by the Secretary of Defense or a DoD Component head that access, under the circumstances, serves the national interest.

d. Congressional staff members requiring access to DoD classified information will be processed for national security eligibility in accordance with this manual.

(1) The Director, WHS, will initiate the required investigation (initial or reinvestigation) to the ISP, adjudicate the results, and grant, deny, or revoke the security eligibility.

(2) The DoD CAF will notify the Assistant Secretary of Defense for Legislative Affairs of the completed eligibility action via the DoD adjudicative system of record. This notification will include only the status of the national security eligibility action; not characterization or details about the action.

e. Staff personnel of a governor's office requiring access to classified information will be investigated and cleared in accordance with the procedures of this manual when the DoD Component head affirms that such eligibility serves the national interest.

f. The Department of Homeland Security is responsible for processing national security eligibility actions for State, local, tribal, and private sector entities in accordance with E.O. 13549, through its State and Local Security Clearance Program on a reimbursable basis, when required by an authorized sponsoring agency. The appropriate Military Department is responsible for processing national security eligibility for State government employees who provide direct support to DoD missions through National Guard elements. DSS is responsible for processing contractor clearances for State, local, tribal, and private sector entities when access to classified information is required in accordance with E.O. 12829.

g. Attorneys representing DoD military and civilian personnel who require access to DoD classified information to properly represent their clients will normally be investigated by the DoD ISP and cleared in accordance with standard procedures for the required level of access.

(1) The General Counsel or Judge Advocate General of the DoD Component involved in the litigation (as applicable for matters under their cognizance) will certify that attorney access to specified classified information is necessary to adequately represent the client.

(2) In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of this section, access may be granted with the written approval of an authority designated in Appendix 1 to Section 7 of this manual, provided that, at a minimum:

(a) A favorable FBI name check and FBI fingerprint check have been completed.

(b) An SF 312, "Classified Information Nondisclosure Agreement," or other non-disclosure agreement approved by the DNI has been executed consistent with Volume 1 of DoD Manual (DoDM) 5200.01.

(c) The appropriate PSI has been requested.

(3) In post-indictment cases, after a judge has invoked the security procedures of Appendix 3 to Title 18, U.S.C., the Department of Justice may elect to conduct the necessary national security investigation and issue the required security clearance, in coordination with the affected DoD Component.

h. Attorneys representing contractor personnel who require access to DoD classified information to properly represent their clients will normally be investigated and cleared in accordance with Title 18, U.S.C.

SECTION 5: INVESTIGATIVE REQUESTS

5.1. GENERAL.

a. Only the authorities designated in this section will submit investigative requests. These authorities will be held responsible for determining if personnel under their jurisdiction require a PSI.

b. Before requesting a new investigation, DoD Components must determine whether reciprocity applies, as outlined in Appendix 5A.

c. The sponsoring DoD activity is responsible for funding all PSIs except for contractor personnel.

d. Investigative requests for contractor personnel under the NISP are processed in accordance with DoD 5220.22-M.

5.2. AUTHORIZED REQUESTORS. Requests for PSIs will be accepted only from designated officials with an approved submitting office number (SON) within the:

a. Military Departments.

b. Office of the Chairman of the Joint Chiefs of Staff and the Combatant Commands.

c. DoD CAF.

d. Defense Agencies and DoD Field Activities.

e. OSD.

f. Other requestors approved by the DDI(I&S).

5.3. LIMITATIONS AND RESTRICTIONS FOR SUBMITTING INVESTIGATIONS.

a. Authorized Personnel Security Investigative Agencies. E.O. 13467 established the DNI as the Security Executive Agent (SecEA) and the final authority to designate agencies to conduct investigations of persons who are proposed for national security eligibility. Only DoD Components delegated investigative authority by the DNI through USD(I&S) may enter into contracts to conduct PSIs. DoD Components without investigative authority are prohibited from entering into contracts to conduct PSIs.

b. Limits on Investigations. Personnel who are employed by or serving in a military, civilian, contractor, or consultant capacity may be considered for national security eligibility only when such eligibility is required for a lawful and authorized government purpose in connection with official duties. The number of persons requiring investigations and national

security eligibility will be limited to those that are essential to current operations and clearly authorized by DoD policy.

(1) Unauthorized, unnecessary, or duplicative PSIs are prohibited. An investigation will not be requested when there is no requirement.

(2) DSS will not process a PSI request for an employee of, or a consultant to, a contractor when there is not a legitimate requirement for access to classified information in supporting a U.S. Government or foreign government requirement in accordance with Volume 2 of DoDM 5220.22 and Volume 3 of DoDM 5200.22.

(3) Spouses of GO/FOs will not be processed for eligibility for access to classified information unless there is need for them to access classified information as part of a unit support or readiness function.

(4) With the exception of military personnel, minors who are under the age of 18 will not be investigated nor granted national security eligibility.

5.4. PROCESSING INVESTIGATIVE FORMS.

a. An investigative request must be submitted early enough to allow sufficient time to complete the investigation, adjudicate the findings, and make the eligibility determination. To conserve investigative resources and ensure investigations are efficient, complete, and thorough, organizations requesting investigations will:

(1) Ensure request forms, prescribed documentation and fingerprints are properly executed and submitted electronically in accordance with ISP instructions. The electronic submission of fingerprints eliminates the need to request advance fingerprint results.

(2) Only request Advance National Agency Check Status Reports when a subject requires Interim TS.

(3) Submit investigative requests for contractor personnel under the NISP through JPAS to the DSS Personnel Security Management Office for Industry to determine validity of the request and process for interim eligibility, as appropriate, and release to OPM.

(4) Promptly notify the ISP if the investigation is no longer needed.

b. To be more efficient, before submitting PSI requests, DoD Components should:

(1) Ensure the investigative requirements, as specified in Section 4 of this manual, are accurately recorded in appropriate systems. This data will be used for programming and to validate electronic PSI requests.

(2) For individuals who are born outside the United States, enter extra coverage codes on the investigative request forms to require OPM to validate citizenship in accordance with national standards. DoD Components should also review citizenship documents of individuals

born abroad before submitting initial PSI requests. All documents verifying U.S. citizenship will be original or certified copies. A copy of the document(s) used to verify citizenship will be uploaded to the subject's electronic Questionnaire for Investigations Processing (e-QIP) before submission to the ISP.

(a) Acceptable Documentation for U.S. Citizenship by Birth. Subjects asserting U.S. citizenship by birth will provide:

1. A birth certificate certified with the registrar's signature that bears the raised, impressed, or multicolored seal of the registrar's office.

2. A Department of State (DOS) Form FS-240, "Consular Report of Birth Abroad of a Citizen of the United States of America."

3. A DOS Form FS-545 or DS-1350, "Certification of Birth."

4. A valid U.S. passport, unaltered, originally issued to the subject.

(b) Acceptable Documentation for U.S. Citizenship by Certification or Naturalization. Subjects asserting citizenship by certification or naturalization will provide:

1. A U.S. Citizenship and Immigration Services (USCIS) Form N-560 or N-561, "Certificate of U.S. Citizenship."

2. A USCIS Form 550, "Certificate of Naturalization" or 570, "Replacement Certificate of Naturalization." Copies can be made of naturalization papers for submission in accordance with Section 1426 of Title 18, U.S.C.

3. A valid U.S. passport or passport card, unaltered, originally issued to the subject.

(c) Acceptable Documentation for Corroboration of Legal Status. These documents or any successors to these forms can be used to corroborate a person's legal status:

1. A valid USCIS Form I-551, "Permanent Resident Card or Resident Alien Card."

2. A U.S. Customs and Border Protection Form I-94, "Arrival/Departure Record," with an acceptable visa that authorizes employment in the United States.

3. A valid USCIS Form I-766, "Employment Authorization Document."

4. A valid U.S. Travel Document issued as a Permit to Re-enter (USCIS Form I-327) or as a Refugee Travel Document (USCIS Form I-571).

c. Investigative requests will be submitted to the ISP through electronic application. The methods for submitting investigative requests to OPM are detailed in the U.S. Office of Personnel Management Booklet. The trained official submitting the request will:

(1) Use the DoD electronic system of record for investigation and adjudication status to verify whether an individual has an open case or an existing investigation that meets the eligibility requirement before submitting a new request (do not submit duplicate investigation requests).

(2) Provide the subject with instructions for completing the e-application and assist the subject as necessary.

(3) Document efforts to validate and verify the required information, where appropriate, and maintain documentation in accordance with applicable record retention requirements.

(4) Ensure that all documents are completed in accordance with the instructions of the ISP.

(5) Use the assigned SON and security office indicator (SOI).

(a) The head of the submitting office may authorize individuals to use the SON to obtain information on the case status of a background investigation from the ISP, if the caller can answer the questions asked by the ISP's telephone liaison.

(b) The SOI is used to identify the appropriate official who will receive case results, data, or other information from OPM. Security offices designate security office employees who may contact the ISP to obtain detailed information about a case. Approved employees are the only individuals who may receive information by telephone or secure e-mail. Requests for SOIs for national security investigations must be approved by the DDI(I&S).

d. Provide relevant data concerning the subject of the investigation to the ISP. The subject of each PSI will provide the personal information required by the ISP and DoD 5400.11-R. At a minimum, the subject will:

(1) Provide accurate and complete data as part of the investigation.

(2) Complete the appropriate investigative forms through e-application and electronic fingerprint capture devices.

(3) Execute signed releases, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records to provide relevant record information to the ISP.

(4) Unfreeze any credit or consumer freezes to allow an investigation of credit history. A credit history is a required component of all national security background investigations. If a "freeze" or other administrative hold is placed on the subject's consumer or credit report file, the ISP will not be able to obtain a copy of the report, which can adversely affect eligibility for a national security position.

(a) Anyone with a credit freeze in place should contact the applicable bureau(s) and request the freeze be lifted for a period of 40 days to allow for their background investigation. Make the request when the investigative application is submitted.

(b) The subject will bear any costs associated with lifting the freeze.

e. Strict adherence to the following procedures will significantly reduce rejected investigation requests and facilitate the processing and scheduling of those requests by the ISP:

(1) Match personally identifying data on the electronic fingerprint, releases, certification page, and the e-application **exactly**.

(2) Ensure the subject of the investigation signs and dates each document submitted to the ISP.

(3) Ensure the subject of the investigation recertifies the e-application for changes made on any of the documents listed in Paragraph 5.4.e.(1) that are submitted to the ISP for processing.

f. When an individual cannot make corrections due to deployment, illness, or other similar circumstance, the Federal Investigations Processing Center Form 391, "Certificate of Amended Investigation," (or other approved form) may be used. Federal Investigations Processing Center Form 391 is not for administrative corrections. It is used when substantive changes are made to an individual's e-QIP, and must be signed and certified by the DoD employee making the changes on the individual's behalf.

5.5. TEMPORARY (OR INTERIM) NATIONAL SECURITY ELIGIBILITY.

Unless otherwise prohibited by policy, an individual may be granted temporary national security eligibility pending investigation and a final determination when official functions must be performed before completion of the investigation and adjudication process. See Section 4 for additional information on temporary or interim national security eligibility.

5.6. ONE-TIME OR SHORT DURATION ACCESS.

Circumstances may arise where an urgent operational or contractual need exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than is currently authorized. In many instances, the processing time required to upgrade the national security eligibility would prevent timely access to the information. Section 5 of this manual details the procedures for one-time or short duration access.

5.7. ACCOUNTABILITY OF PERSONNEL SECURITY REPORTS AND RECORDS.

a. Personnel security data, reports, records, and investigative results must be handled with the highest degree of discretion. Access to such information is afforded only for the purposes in the applicable Privacy Act System of Record Notice (SORN) and to persons whose official duties require such information. PSI results may be used only to determine national security eligibility requiring such investigation and for quality assurance, law enforcement investigations, authorized CI inquiries and investigations, and other official uses stated in the applicable SORN or as authorized by DoD 5400.11-R .

b. Internal controls will be established to ensure personnel security data, reports, records, and investigative results are adequately safeguarded and access is limited to official duties by authorized personnel.

(1) Personnel Submitting the E-application. The submitter will maintain a file for each subject who has successfully begun an investigation. Any information verified by the submitter will be maintained in the file until final eligibility is determined.

(2) Adjudication Facilities and DoD Components. Adjudication facilities and the DoD Components will control and maintain accountability of all reports of investigations received, to include supporting documentation.

(a) Unclassified PSI information that is privacy information is treated as For Official Use Only information and handled in accordance with DoD 5400.11-R, DoDM 5400.07, and DoDI 5200.48. Classified PSI information will be protected in accordance with Volume 3 of DoDM 5200.01.

(b) In addition to the requirements cited in Paragraph 5.7.b.(2)(a), when an original classification authority classifies PSI information, it will be handled in accordance with the respective classification guide.

(c) Access to national security eligibility determination information will be made available only to officials of the DoD and the Federal Government with an official need for such information. Personnel who review and access completed investigation files to render national security eligibility determinations require a favorably adjudicated SSBI.

(d) Reproduction, in whole or in part, of PSI security investigative reports is restricted to the minimum number of copies required for the performance of assigned duties.

(e) Unclassified PSI information is stored in a vault, safe, or steel file cabinet with a built-in lock or an approved three-position dial-type combination padlock or in data bases which are access controlled. When needed for official duties by personnel authorized access, and where supplemental controls are in place, personnel security data, reports, records, and investigative results may be stored in key or cipher-locked rooms or cabinets to which only authorized employees have access.

5.8. SUBJECT REQUEST FOR PSI REPORT.

The subject of investigation will be given access to PSI reports in accordance with E.O. 12968, DoD 5400.11-R and DoDM 5200.01, as applicable.

5.9. RECORDS DISPOSITION.

a. Any personnel security investigative report provided by the ISP may be retained by the DoD Component only for the period identified in its Privacy Act SORN.

b. Destruction will be in accordance with DoD records management policy and the Component's approved records management schedule. Destruction will be accomplished in accordance with DoDM 5200.01 or, if classified, in accordance with the December 12, 2005 Office of Management and Budget Memorandum.

APPENDIX 5A: RECIPROCITY

5A.1. GENERAL.

a. Gaining DoD Components may use this appendix to determine whether an individual has a current national security eligibility, including access to highly sensitive information (i.e., SCI, SAP, or "Q"), based upon the requisite investigation (i.e., ANACI, NACLC, SSBI, or SSBI-PR).

b. E.O. 13467 establishes the DNI as the SecEA responsible for ensuring reciprocal recognition of national security eligibility among the agencies, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of investigations and determinations of national security eligibility.

c. DoD reciprocally accepts existing national security eligibility determinations or clearances from other government agencies in accordance with E.O. 13467 , Part 731 of Title 5, U.S.C., and the December 12, 2005, July 17, 2006, and November 14, 2007 Office of Management and Budget Memorandums.

d. Background investigations and national security eligibility determinations made by designated DoD authorities will be mutually and reciprocally accepted by all DoD Components.

e. Further investigation is prohibited when a determination already exists that is based upon a current investigation of a scope that meets or exceeds that necessary for the eligibility required. See Paragraph 5A.3 for reciprocity exceptions.

f. Reciprocal use of an investigation is based on:

(1) SCI eligibility in accordance with Intelligence Community Directive 704 and Intelligence Community Policy Guidance Numbers 704.1, 704.2, 704.3, 704.4, and 704.5.

(2) Collateral TS and below, or any SAP eligibility-up to 5 years from the close date of the completed PSI.

g. National security and SCI eligibility suspensions, denials, and revocations within DoD will be mutually and reciprocally recognized, provided the opportunity for administrative due process offered by the issuing organization and the gaining organization are the same. This will apply for at least the 12-month period following the date of final denial or revocation of access during which time the individual is ineligible for reconsideration. See Section 6 for reconsideration procedures.

h. Whenever a civilian or Service member transfers from one DoD activity to another, the losing organization's security office will advise the gaining organization of any action to suspend, deny, or revoke the individual's eligibility, as well as any issue information that may exist in security, personnel, or other files. In such instances, the eligibility will not be reissued until the potentially disqualifying information has been adjudicated.

i. When a valid DoD national security eligibility is on record, DoD Components will not request before investigative files for review. See Paragraph 5A.3 for reciprocity exceptions.

j. The gaining activity will **not** require an individual to complete an SF 86 if a valid DoD national security eligibility or access eligibility is on record. However, a completed SF 86C, "Certification," may be requested to determine whether new substantive information of security concern has occurred since the last adjudication. Following review, the SF 86C will be forwarded to the appropriate adjudication facility and added to the individual's adjudicative record.

k. Reciprocal recognition by an activity may be withdrawn on a case-by-case basis if such action is necessary for national security purposes.

5A.2. VERIFY ELIGIBILITY.

a. DoD Components that grant access or issue national security eligibility to civilian, military, or contractor employees are responsible for determining whether such employees have been previously cleared or investigated by the Federal Government. In most circumstances, this can be accomplished by checking OPM's Central Verification System, the DoD adjudication system of record (JPAS or the IC's Scattered Castles database).

b. Receiving activity security personnel may communicate directly with originating activity security POCs to verify that national security eligibilities in question were granted.

c. If online access to the appropriate database is unavailable, or if the record is otherwise incomplete, fax an "Inter-Agency Clearance Verification Request" to the appropriate agency. The request form and appropriate fax numbers can be found at the secure OPM web portal at https://opmis.xsp.org/index.cfm. The OPM Federal Investigative Services Division has created and posted a list of contact information to the "public library" section of its secure portal for all agencies which grant eligibility. Senior security personnel in the DoD Components will designate security personnel who will require access to the OPM web portal.

5A.3. EXCEPTIONS TO RECIPROCITY. The gaining activity or program may request that an individual who has current national security eligibility with another federal agency complete a new security questionnaire, may review existing security questionnaires or background investigations, or may initiate any new investigative checks when:

a. The determination of eligibility for access is based on an exception (e.g., condition, deviation, or waiver) or is granted on an interim or temporary basis.

b. The investigation upon which the existing national security eligibility was granted is not current.

c. The gaining activity is aware or in possession of substantial information indicating the standards in the August 30, 2006 USD(I) Memorandum may not be satisfied.

d. The individual is being considered for access to highly sensitive information (i.e., SCI, SAP, or "Q") and:

(1) The existing national security eligibility determination is based upon a waiver or deviation, or access is otherwise subject to conditions, or

(2) The individual does **not** satisfy a polygraph requirement imposed by the gaining program, as approved by the DoD Component head or head of an IC element. Under such circumstances, only additional, not duplicative, investigative or adjudicative procedures will be completed, or

(3) The individual does **not** satisfy an official requirement imposed by the gaining program that prohibits **any** non-U.S. immediate family or non-U.S. cohabitants. Under such circumstances, only additional, not duplicative, investigative or adjudicative procedures will be completed.

e. There is a break in employment or a break in access greater than 24 months.

5A.4. ANNOTATING RECIPROCAL DETERMINATIONS.

a. To be consistent with reciprocity and to ensure equitable due process, the DoD Components will ensure the timeliness of investigation submissions and adjudications of civilian employees, military, and contractor personnel as required.

b. Once a gaining DoD adjudicative authority confirms or is assured that a previous investigation meets the provisions of this section and accepts the losing organization's determination, the reciprocally accepted determination will be entered into the DoD adjudication system of record.

c. If eligibility determinations are based on an exception (condition, deviation, or waiver), mitigating conditions must be annotated in the DoD adjudication system of record.

d. DoD Components will provide eligibility and access determination information to other agencies of the Federal Government to which an individual is assigned or detailed, upon request.

5A.5. ADDITIONAL RECIPROCITY GUIDANCE FOR SCI ACCESS. When a determination of eligibility for access is based on an exception (i.e., condition, deviation, or waiver) that information will be conveyed to the gaining head of an IC element. The gaining head of an IC element may reject another head of an IC element access determination based upon his or her assessment of risk.

5A.6. RECIPROCITY FOR THE NUCLEAR REGULATORY COMMISSION AND THE DOE. DoD policy on reciprocal acceptance of security eligibility with the Nuclear Regulatory Commission and the DOE is established in Table 1 of DoDI 5210.02.

SECTION 6: LAA FOR NON-U.S. CITIZENS

6.1. GENERAL. Only U.S. citizens are eligible for access to classified information. However, compelling reasons may exist for granting access to classified information to a non-U.S. citizen. An LAA enables a non-U.S. citizen to have limited access to classified information, but the LAA is **not** a national security eligibility.

a. An LAA may be granted, in rare circumstances, when:

(1) A cleared or clearable U.S. citizen is not readily available or does not possess the skills or expertise required.

(2) The non-U.S. citizen possesses unique skills or expertise needed to support a specific U.S. Government requirement involving access to classified information.

b. Access to classified information provided to the U.S. Government by another government or international organization will not be permitted under an LAA without written consent of the government of the organization that provided the information.

c. All LAAs will be reviewed annually to determine if continued access is in compliance with DoD policy. The DoD Components will maintain a record of all LAAs in effect and submit an annual report to the Office of the DDI(I&S) by January 15 for the preceding year providing a summary by access level (Secret or Confidential), country(ies) of citizenship, and employment location.

6.2. CONDITIONS FOR LAA.

a. An export license or disclosure authorization is required to release classified information to a non-U.S. citizen who has been issued an LAA. Before submitting an application for an LAA, the requestors must obtain a written disclosure determination from a principal or designated disclosure official or obtain a DOS approved export license. This documentation must be submitted with the application for an LAA. The LAA cannot serve as an export authorization. An approved LAA is a determination that the non-U.S. citizen is eligible to receive the classified information governed by the disclosure authorization or DOS approved export license.

b. Personnel granted LAAs are not permitted uncontrolled access to areas where classified information is stored or discussed. Classified information will be maintained in a location under the continuous control and supervision of an appropriately cleared U.S. citizen.

c. Non-U.S. citizens will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be released to the country of which the person is a citizen, but not to exceed the Secret level.

d. Personnel granted LAAs will not be designated as a courier or escort for classified material unless they are accompanied by an appropriately cleared U.S. citizen.

6.3. INVESTIGATIVE REQUIREMENTS.

a. A non-U.S. citizen, including immigrant alien, may be issued an LAA if:

(1) The individual is a citizen of a country with which the United States has an agreement providing for security assurances.

(2) The investigative requirements for the LAA are commensurate with the investigative requirements of that country.

b. A favorably completed and adjudicated SSBI (within the immediately preceding 5 years) is required before granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no applicable host country prohibitions) to resolve the remaining personnel security issues will be favorably completed in accordance with DoDD 5210.48 before granting access.

c. If geographical, political, or medical situations prevent the full completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, an LAA may be granted only with approval of the DDI(I&S).

d. If an LAA is withdrawn and the person subsequently is again considered for a new LAA, an SSBI and polygraph examination may be required. The scope of the SSBI will cover the period since the previous investigation or 10 years, whichever is shorter.

e. A PR will be conducted on every person with an LAA 5 years from the closing date of the previous SSBI or SSBI-PR, as appropriate.

6.4. AUTHORIZED ACCESS LEVELS.

a. LAAs may be granted only at the Secret and Confidential levels. Limited access to Secret and Confidential information may be granted following completion of the SSBI by an authority as specified in Section 4 of this manual, and compliance with the requirements in this section.

b. The classified information to which the non-U.S. citizen may have access will be approved for release to the person's country (or countries) of citizenship, in accordance with DoDD 5230.11. Exceptions may apply in operational exigencies. In such cases, the DoD Component head may approve the release of information to individuals granted an LAA when it is determined to be in the best interests of national security.

c. Access to classified information will be limited to a specific program or project. The LAA will be cancelled upon completion of the program or project for which it was approved.

d. Foreign nationals of a NATO member nation may be authorized access to NATO information provided:

(1) A NATO Security Clearance Certificate is obtained by the CSA from the individual's home country.

(2) NATO access is limited to performance on a specific NATO program or project.

e. Access to classified information outside the scope of the approved LAA will be considered a compromise of classified information and investigated in accordance with the November 15, 2007 Office of Management and Budget Memorandum.

f. Access by foreign nationals to DoD information systems containing classified information will comply with conditions prescribed in DoDI 8500.01.

6.5. UNAUTHORIZED ACCESS LEVELS. An LAA granted under the provisions of this manual is not valid for access to:

a. TS information.

b. Restricted data (RD) or formerly restricted data.

c. Information that has not been determined releasable by a U.S. Government designated disclosure authority to the country(ies) of which the individual is a citizen.

d. Communications security (COMSEC) information.

e. Intelligence information.

f. Information for which foreign disclosure has been prohibited in whole or in part.

g. Information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

6.6. REQUEST PROCEDURES.

a. Personnel being processed for an LAA will complete an SF 86.

b. In those instances where a non-U.S. citizen does not have an social security number, follow the procedures specified by the ISP when completing the SF 86.

c. All requests for initial LAAs will contain a detailed justification and plan describing:

(1) The location of the classified material (security containers) in relationship to the location of the foreign national.

(2) The compelling reason for not employing a cleared or clearable U.S. citizen.

(3) A synopsis of an annual continuing assessment program to evaluate the individual's continued trustworthiness and eligibility for access.

(4) A plan to control access to secure areas and to classified and controlled unclassified information.

d. All LAA determinations, favorable and unfavorable, will be entered into the DoD adjudication system of record.

e. Unfavorable LAA determinations for industrial contractor personnel are processed pursuant to DoDD 5220.6.

6.7. LAA DETERMINATION AUTHORITY.

a. LAA determinations will be made by a designated single authorizing adjudicative official listed in Section 4 of this manual. LAA determination authority will not be further delegated to any other official at the major command level or equivalent. An LAA requested by a contractor under the NISP will be endorsed by the program executive officer or equivalent official responsible for the contract under which the request has been submitted in accordance with DoD 5220.22-M. An LAA will not be issued in the absence of such an endorsement.

b. The Combatant Commander responsible for implementation of the PSP is authorized to issue, deny, or revoke an LAA. LAA determinations by the Combatant Commanders will be reported to the DoD CAF in accordance with the assigned responsibilities in DoDD 3700.01 for inclusion in the DoD system of record.

SECTION 7: NATIONAL SECURITY ADJUDICATIONS

7.1. GENERAL.

a. The principal objective of the DoD personnel security adjudicative function is to ensure individuals who are granted national security eligibility are reliable, loyal, and trustworthy. It involves an assessment of a sufficient portion of their life history to determine whether they have acted or are acting in ways inconsistent with the adjudicative guidelines. Cases are evaluated using uniform national standards to ensure fair and consistent assessments. Adjudications are performed to determine an individual's eligibility for access to classified information or to hold a sensitive position.

(1) National security eligibility determinations are a function distinct from granting access to classified national security information. This section provides procedures relating to determining national security eligibility. Section 5 of this manual provides procedures for access determinations.

(2) National security **eligibility** determinations are made on the merits of the individual case and involve examining a sufficient period of a person's life and background to make an affirmative determination the person is an acceptable national security risk (i.e. where the facts and circumstances indicate granting eligibility is clearly consistent with the national security interests of the United States). Favorable **access** determinations are made on the basis of the eligible individual's need for access to classified information to perform official duties.

b. All reliable information relevant to determining whether a person meets the national security eligibility standards is reviewed and evaluated only by appropriately trained adjudicative personnel, in accordance with appropriate procedures approved by the SecEA. Final adjudication determinations will be made by certified adjudicators, non-certified adjudicators operating under an approved risk management plan, or in accordance with approved automated procedures.

7.2. ADJUDICATION AUTHORITIES.

a. Only the determination authorities listed in Appendix 7A are authorized to make national security eligibility determinations based upon a review of the PSI or adverse information referral.

b. Re-adjudication by any DoD Component of national security eligibility determinations for individuals who have been determined to be eligible by the DoD CAF, by another DoD Component, or by another federal agency is prohibited except in accordance with Appendix 5A.

c. SCI access eligibility determinations follow Volume 2 of DoDM 5220.22 and associated DNI guidance and delegations.

7.3. PROHIBITION ON RETALIATION BY AFFECTING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION.

a. It is strictly prohibited to take, fail to take, or threaten to take or fail to take any action affecting an individual's eligibility for access to classified information as a reprisal for a protected disclosure of fraud, waste, or abuse pursuant to Presidential Policy Directive/PPD 19.

b. Employees may appeal actions affecting eligibility for access to classified information allegedly taken as a reprisal for a protected disclosure of fraud, waste, or abuse in violation of Presidential Policy Directive/PPD 19.

c. All personnel security adjudicators, DOHA administrative judges (AJs), and Personnel Security Appeals Boards (PSABs) will, as part of their adjudication of an individual's eligibility, consider and resolve any claims of reprisal for whistleblowing.

d. Nothing in this manual limits or affects the independence of the Inspector General of the Department of Defense or the DoD Component statutory Inspector Generals in fulfilling their duties to determine whether an action affecting eligibility for access to classified information constituted a prohibited reprisal and to recommend appropriate corrective action to the DoD Component head.

7.4. ADJUDICATIVE GUIDELINES. The adjudicative guidelines will be used to determine an individual's national security eligibility. These guidelines are national level guidelines developed and distributed by the December 29, 2005 White House Memorandum, Intelligence Community Policy Guidance 704.2, or their successor documents, as appropriate.

7.5. ELECTRONIC ADJUDICATION (E-ADJUDICATION).

a. Use of automated adjudication procedures for e-adjudication is restricted to authorized adjudication facilities.

b. All determinations made by authorized adjudication facilities using approved e-adjudication business rules are valid and will be recorded in JPAS and accepted on a reciprocal basis.

7.6. ADJUDICATION OF NATIONAL SECURITY CASES.

a. PSIs may be adjudicated by e-adjudication using DNI-approved business rules, by certified adjudicators who have successfully completed the standards for experience, training, and certification to perform final adjudicative determinations, or by non-certified adjudicators operating under an approved risk management plan in accordance with the January 28, 2014 USD(I) Memorandum, DoDI 3305.13, and DoD 3305.13-M.

b. All military positions are national security positions regardless whether or not the Service member requires access to classified information, as established in DoDI 5200.02.

(1) All military members will undergo PRs, maintain a favorable adjudication, and be subject to continuous evaluation.

(2) All military members will undergo the NACLC or successor Tier 3 investigation at a minimum. The DoD CAF will adjudicate all military investigations and reinvestigations using the national security adjudicative guidelines.

(a) Military members who are denied or revoked a favorable national security eligibility determination will be afforded due process. Those individuals will be immediately referred to the servicing Military Department for appropriate action.

(b) Military members who are determined to be ineligible for access to classified material solely because of citizenship will be entered into JPAS as not eligible for access to classified material.

7.7. DOD CASE MANAGEMENT AND ADJUDICATION TRACKING SYSTEMS. The Case Adjudication Tracking System (CATS), National Security Agency/Central Security Service's Clearance Workflow and Verification System as authorized by the April 10, 2009 USD(I) Memorandum or the Defense Intelligence Agency (DIA) Total Integrated Team Analysis Network are DoD information technology systems capable of receiving national security investigations, managing workflow, and performing electronic adjudications.

7.8. DOCUMENTING ADJUDICATIONS.

a. Adjudicative determinations, whether favorable or unfavorable, interim or final, will be entered into JPAS on the same day the determination is made.

b. When derogatory information is not obviously and clearly mitigated by a mitigating condition, the disqualifying and mitigating condition(s) from the applicable adjudicative guideline and the rationale for each decision will be recorded in JPAS.

c. Applicable adjudication rationales will be documented in accordance with the August 31, 2010 USD(I) Memorandum.

d. All records will indicate whether an exception (condition, deviation, or waiver), as defined in Intelligence Community Directive Number 704, or a Bond Amendment waiver as detailed in Appendix 7B.3.e. was used to make an eligibility determination.

7.9. PERSONNEL PERFORMING ADJUDICATIVE FUNCTIONS. Adjudicative determinations are inherently governmental functions. However, the DoD CAF and DoD IC central adjudication facilities may contract for adjudicative support services to ensure timely accomplishment of mission objectives.

a. Inherently Governmental Functions. Government personnel who use contract support remain responsible for ensuring the completeness and accuracy of the case file and for

considering all material submitted therein in their adjudicative decision. Government personnel will:

(1) Retain the authority and responsibility for making discretionary decisions, value judgments inherent in adjudication, and all final adjudicative determinations.

(2) Conduct all adjudicative services and functions in cases involving LAA, and requests for security assurance submitted by foreign governments for U.S. citizens requiring access to foreign government information.

b. Contractor Personnel Support of Adjudications. Services that may be provided by contractor personnel include administratively processing cases to ensure expeditious case management, pre-screening cases for investigative compliance, and other support that is ministerial in nature. Contract services cannot be so extensive as to exceed the capacity of Component oversight or limit the opportunity for proper discretionary decisions and value judgments by government adjudicative personnel.

(1) Contractor personnel providing adjudicative support must meet the same eligibility and investigative requirements required of government personnel with comparable duties.

(2) Adjudication contractor support personnel will be subject to continuous review by the appropriate DoD CAF or DoD IC central adjudication facility personnel (e.g., the Contract Officer's Representative) for contract compliance and will work only at adjudication facility-approved locations.

7.10. SCI ADJUDICATION.

a. SCI adjudication policy and guidelines are contained in Intelligence Community Directive 704 and Intelligence Community Policy Guidance 704.2.

b. SCI adjudication and eligibility determinations will be made in accordance with Intelligence Community Policy Guidance Numbers 704.1, 704.2, 704.3, and 704.4. SCI eligibility determinations include TS eligibility and below.

c. SCI adjudications of PSIs by the DoD CAF or applicable IC adjudication facilities will be limited to personnel affiliated with, assigned to, or under contract with the Component the central adjudication facility supports or with whom special agreements exist to provide SCI adjudication.

d. The applicable IC adjudication facility will notify the DoD CAF when they remove an individual under the DoD CAF's cognizance from SCI access.

e. When SCI access is removed from an individual for adverse reasons, the DoD CAF will review the adverse information and make a separate collateral eligibility determination. If an SCI access is removed for contractor personnel cleared through the NISP, the Director of DSS, in coordination with the DoD CAF, will advise the contractor if loss of SCI access also warrants withdrawal of collateral eligibility.

7.11. SAP ADJUDICATION.

a. SAP nomination policy and guidelines are contained in the May 20, 2013 USD(I) Memorandum.

b. SAP adjudication and continued eligibility determinations will be made in accordance with DoDD 5205.07 and the August 9, 2011 USD(I) Memorandum.

c. The applicable SAP Central Office will notify the DoD CAF when adverse reasons warrant the removal of an individual from SAP access.

d. When SAP access is removed from an individual for adverse reasons, the servicing adjudication facility will review the adverse information and determine whether SCI access or collateral eligibility should be withdrawn. If SAP access is removed for contractor personnel cleared through the NISP, the Director, DSS, in coordination with the DoD CAF, will advise the contractor when to remove SCI access or collateral access.

7.12. POLYGRAPH AND CREDIBILITY ASSESSMENT PROCEDURES.

a. The use of polygraph and other approved credibility assessment tools is governed by DoDI 5210.91.

b. Except as authorized by DoDI 5210.91, no unfavorable national security eligibility determination will be taken based solely on a polygraph examination that is interpreted as indicating deception or is inconclusive. Refusal to take a voluntary polygraph will be given no consideration, favorable or unfavorable, when making a national security eligibility determination.

c. Admissions made during the polygraph interview or attempts to employ countermeasures to defeat a polygraph may be considered when making a national security eligibility determination.

7.13. ADJUDICATION TIMELINES. DoD adjudications will be completed in accordance with standards established by the SecEA and as required by Title 50, U.S.C.

7.14. DURATION OF SECURITY ELIGIBILITY AND ACCESS DETERMINATIONS.

The validity of national security eligibility and access determinations is not limited to a specific duration in years, except as prescribed in this section.

a. Security clearance eligibility and access do not expire simply because of an overdue PR as long as the individual submitted required paperwork or operational factors (such as deployment) or DoD Component decisions (such as funding constraints) delay submission. When the circumstances precluding on time submission are gone, DoD Components must submit PRs as soon as practicable.

b. Individuals who received a favorable adjudication of an investigation within the previous 5 years from the date the investigation closed and who have been retired or otherwise separated from U.S. Government employment for no more than 24 months will be granted eligibility as long as:

(1) There is no indication the individual no longer satisfies the standards established for access to classified information.

(2) The individual certifies in writing on an SF 86C to the security professional there has been no change in the relevant information provided for the last background investigation. The SF 86C will be forwarded to the DoD CAF and added to the individual's adjudicative record.

(3) An appropriate record check reveals no unfavorable information.

c. Commands may determine the submission of a new background investigation is merited when the SF 86C reveals derogatory information.

d. In all instances, if the most recent previous determination issued to the individual was a revocation, denial, or suspension, re-adjudication will be required.

7.15. DETERMINING ELIGIBILITY WITH CONDITIONS.

a. The presence of derogatory information or information that raises a security concern does not necessarily mean adjudicators will not grant or continue an individual's national security eligibility.

b. Adjudicators may issue favorable determinations or continue an individual's eligibility with conditions. An individual's failure to comply with the condition(s) or warning(s) may result in revocation of national security eligibility.

c. The local security professional will monitor individuals granted eligibility based on conditions and report the results to the supporting central adjudication facility semi-annually until the conditions are removed.

d. Adjudicators must document eligibility determinations issued with conditions in JPAS and revisit the determination annually until the conditions are removed.

7.16. INTERIM ELIGIBILITY.

a. Individuals may be granted temporary eligibility where official functions must be performed before completion of the national security investigation and adjudication process. Within the DoD temporary eligibility is referred to as "interim eligibility" or "interim."

(1) The authorities listed in Appendix 7A to this section may grant interim eligibility to personnel under their administrative jurisdiction pending a final national security eligibility determination by the adjudication facility. Only government personnel may make interim

determinations. Justification for interim eligibility will be recorded in JPAS and the employee must be notified in writing by their employing activity that further access is expressly conditioned upon the completion of the national security investigation and granting of national security eligibility in accordance with national security adjudicative guidelines in the August 30, 2006 USD(I) Memorandum.

(2) Interim eligibility will be valid for up to 1 year. A 6 month extension may be made by the designated Component authority if:

(a) The national security investigation has not been completed due to deployment.

(b) The eligibility determination is pending at the central adjudication facility.

(3) The DoD Component will notify the adjudication facility of the extension via JPAS entry.

(4) The DoD Components will monitor all interims more than 1 year old to ensure:

(a) The national security investigation is ongoing.

(b) The individual still requires access.

(5) The adjudication facility will update JPAS to reflect the withdrawal of interim eligibility after 1 year or after the expiration of an approved 6-month extension.

b. Minimum requirements for interim Confidential or Secret eligibility are:

(1) Acceptable proof of citizenship.

(2) Favorable review of a completed SF 86.

(3) Favorable review of local personnel, base, military police, medical, and security records, as applicable.

(4) An appropriate national security investigation opened by the ISP.

(5) Favorable review of FBI Criminal History Report (fingerprint results).

c. Minimum requirements for interim TS eligibility are:

(1) Favorable completion of all requirements cited for interim Secret or Confidential eligibility.

(2) Favorable completion of a National Agency Check.

d. The authorities listed in Appendix 5A to this section may withdraw an interim eligibility at any time if and when they determine that the granted interim poses an unacceptable risk.

e. An interim Secret or Confidential is valid for access to the level of eligibility granted. Access to RD, COMSEC information, and NATO information is not authorized.

f. An interim TS is valid for access to TS information, and RD, COMSEC, and NATO information at the Secret and Confidential level.

g. Interim access to SCI information is determined by the access granting authority.

h. Interim eligibility for contractor personnel under the NISP is governed by DoD 5220.22-M.

i. The DNI provides guidance for temporary eligibility for SCI in Intelligence Community Directive Number 704.

j. Interim eligibility determinations and access are prohibited for National Security Agency/Central Security Service assignment, detail, or employment in accordance with DoDI 5210.45.

k. Eligibility determinations for SAP access are governed by DoDD 5205.07, DoDI 5210.91, and the August 9, 2011 USD(I) Memorandum.

APPENDIX 7A: DETERMINATION AUTHORITIES

7A.1. OFFICIALS AUTHORIZED TO GRANT, DENY, REVOKE, OR SUSPEND NATIONAL SECURITY ELIGIBILITY. Inherent in this authority is the ability to make interim access determinations.

a. Secretary of Defense.

b. CMO.

c. Director, DIA.

d. Director, National Geospatial-Intelligence Agency (NGA).

e. Director, National Reconnaissance Office (NRO).

f. Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

g. GC DoD (for contractor personnel under the NISP) through DOHA.

h. Secretary of the Army.

i. Secretary of the Navy.

j. Secretary of the Air Force.

k. Chairman of the Joint Chiefs of Staff and Combatant Commanders.

l. This authority may be further delegated in writing to the extent necessary by the officials listed in Paragraphs 7A.1.a through 7A.1.k.

m. Director, DSS is authorized to grant interim clearance eligibility for NISP contractor personnel under DSS cognizance and to suspend eligibility. DSS is not authorized to deny or revoke national security eligibility.

7A.2. OFFICIALS AUTHORIZED TO SUSPEND ACCESS TO CLASSIFIED INFORMATION.

a. Commanders, DoD Component heads, or adjudicative authorities.

b. For SCI, cognizant heads of IC elements.

c. For SAP information, Special Access Program Central Office.

d. DSS for cleared NISP contractor personnel under DSS cognizance in accordance with the standard in DoDD 5220.6.

e. The authority to suspend access to classified information or occupy a national security position may be further delegated in writing to appropriate subordinates by the officials listed in Paragraph 7A.1.

7A.3. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA.

a. CMO or single designee.

b. Director, DIA or single designee.

c. Director, NGA or single designee.

d. DIRNSA/CHCSS or single designee.

e. Director, NRO or single designee.

f. Secretary of the Army or single designee.

g. Secretary of the Navy or single designee.

h. Secretary of the Air Force or single designee.

i. Chairman of the Joint Chiefs of Staff or single designee.

j. Combatant Commanders or single designee.

7A.4. FINAL DETERMINATIONS. A three-member PSAB panel will be formed to render final determinations when an unfavorable national security determination is appealed. PSABs may be established under:

a. Secretary of the Army.

b. Secretary of the Navy.

c. Secretary of the Air Force.

d. DIRNSA/CHCSS.

e. Director, DIA.

f. Director, NGA.

g. Director, NRO.

h. Director, WHS.

i. GC DoD

APPENDIX 7B: SPECIAL CIRCUMSTANCES

7B.1. ADHERENCE TO FEDERAL LAWS.

a. This appendix addresses special circumstances that warrant inclusion to ensure compliance with federal law in the execution of the DoD PSP. The PSP specifies that eligibility for access to classified information or assignment to sensitive duties will be granted only to individuals whose personal and professional history affirmatively indicates willingness and ability to abide by regulations governing the use, handling, and protection of classified information. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. E.O. 12564 requires a drug-free federal workplace. The possession of illegal drugs is unlawful under Chapter 13 of Title 21, U.S.C.

7B.2. ADHERENCE TO FEDERAL LAWS PROHIBITING MARIJUANA USE. In accordance with the October 25, 2014 DNI memorandum, agencies are prohibited from granting or renewing a security clearance to an unlawful user of a controlled substance, which includes marijuana. Legislative changes by some States and the District of Columbia do not alter federal law or existing national security guidelines.

7B.3. PROHIBITION FOR ALL SECURITY CLEARANCES (THE "BOND AMENDMENT PROHIBITION").

a. Pursuant to Section 3343 of Title 50, U.S.C. (also known and referred to in this manual as the "Bond Amendment"), federal agencies are prohibited from granting or renewing a security clearance for any individual who is an unlawful user of a controlled substance or is an addict; this prohibition applies to all clearances.

b. For purposes of the Bond Amendment prohibition:

(1) An unlawful user of a controlled substance is any person who uses a controlled substance and has lost the power of self-control with reference to the use of the controlled substance or who is a current user of the controlled substance in a manner other than as prescribed by a licensed physician. Such use is not limited to the use of drugs on a particular day, or within a matter of days or weeks before, but rather that the unlawful use occurred recently enough to indicate the individual is actively engaged in such conduct.

(2) An addict of a controlled substance is any individual who habitually uses any narcotic drug so as to endanger the public morals, health, safety, or welfare; or is so far addicted to the use of narcotic drugs as to have lost the power of self-control with reference to his or her addiction.

c. Pursuant to the Bond Amendment, DoD Components may not, absent a waiver, grant or renew security clearances that provide access to SAPs, SCI, or RD for an individual who has been:

(1) Convicted in any U.S. court of a crime, sentenced to imprisonment for that crime and, as a result incarcerated for not less than 1 year;

(2) Discharged or dismissed from the Military Departments under dishonorable conditions; or

(3) Determined to be mentally incompetent by an adjudicating authority, based on an evaluation by a duly qualified mental health professional employed by, or acceptable to and approved by, the U.S. Government and in accordance with established procedures and standards.

d. Waiver procedures:

(1) Adjudicators will determine if Bond Amendment criteria apply to the case.

(2) A meritorious waiver may be granted, if appropriate, for one or more of the conditions specified in Paragraph 7B.3. if the adjudicator, using the adjudicative mitigating factors, would have arrived at a favorable decision but for the Bond Amendment disqualification.

(3) If, after applying the appropriate mitigating factors listed in the adjudicative guidelines, the adjudicator determines that a meritorious waiver is not appropriate, eligibility will be denied or revoked with a statement of reasons (SOR) that includes the Bond Amendment. The DoD's established administrative review procedures, including hearing and appeal processes, will be followed in all such cases.

(4) Meritorious waivers will be annotated in JPAS. Adjudicators will provide a detailed justification for the waiver in JPAS.

(5) A meritorious waiver may be granted during any stage of the adjudication or due process. If a tentative denial or revocation has been issued, the meritorious waiver decision will be made by the Director or Deputy Director of the DoD CAF. If a letter of denial (LOD) or letter of revocation (LOR) was issued by the DoD CAF, the final meritorious waiver decision will be made by the head of the PSAB, or by the Director, DOHA, for industry cases.

e. By January 7 of each year, heads of adjudication facilities will submit to the OUSD(I&S) Security Policy and Oversight Division an annual granted waiver report providing a summary of all granted for the preceding calendar year. Each summary will detail:

(1) The applicable section of the Bond Amendment.

(2) The nature and date of the military discharge, dismissal, mental health issue, or criminal offense (as applicable).

(3) Any sentence imposed.

(4) The meritorious circumstance(s) cited in support of the waiver.

f. The DDI(I&S) will submit a final Consolidated Granted Waiver Report when waivers were granted in the previous calendar year to Congress by February 1 in accordance with Title 50, U.S.C.

g. Adjudicators from the following DoD Components may authorize waivers of the Bond Amendment disqualification in cases when the SOR or letter of intent (LOI) has not yet been issued:

(1) DoD CAF.

(2) DIA.

(3) National Security Agency/Central Security Service.

(4) NGA.

(5) NRO.

h. Meritorious waivers issued for the Bond Amendment are not subject to reciprocity.

APPENDIX 7C: ADJUDICATION OF INCOMPLETE NATIONAL SECURITY INVESTIGATIONS

7C.1. GENERAL.

a. Rapid Assessment of Incomplete Security Evaluations is the Department's tool for assessing PSI quality and is part of CATS. Rapid Assessment of Incomplete Security Evaluations will be used by all non-IC groups to evaluate incomplete national security investigations that do not meet the federal investigative standards or lack sufficient information required to adjudicate them.

b. A finished investigation report received by an adjudication facility, or authorized designee, where a minor investigative element has not been met (e.g., missing one character reference), does not necessarily require reopening the investigation; does not preclude favorable adjudication; and does not require an exception (condition, deviation, or waiver), if the other information provided by the individual or developed during the investigation is generally favorable.

c. In circumstances where an investigation report received by the adjudication facility contains insufficient detail to favorably resolve potentially disqualifying information, the adjudication facility may (without re-initiating the investigation) acquire additional information about the individual such as obtaining a medical evaluation or using interrogatories. A copy of information acquired by the adjudication facility will be forwarded to the ISP and appended to the investigative record.

d. Complete investigative information provides the best foundation for the adjudication process. When adjudicators are faced with incomplete reports of investigations that have missing scope item coverage, they must decide whether to return the investigation to the ISP, make a determination despite the missing information, or gather the information themselves. Training and experience provide adjudicators with the background for deciding between these options.

e. Adjudicators may obtain and rely upon official records published (made publicly accessible) by federal, State, or local government.

f. Further guidance in adjudicating investigations that have missing or incomplete information is contained in the July 13, 2010 and March 10, 2010 USD(I) Memorandums.

7C.2. FACTORS TO CONSIDER. A decision about whether to return an investigation with missing or incomplete scope items is a risk management decision that requires adjudicators to use their best judgment to weigh many factors when evaluating an investigation. These factors include:

a. Explanations for Missing or Incomplete Scope Items. Investigator notes documenting why items are missing or incomplete can help adjudicators decide whether to make a

determination despite missing information. When investigators cannot obtain the required coverage in a case, they must document the efforts expended and the reasons for the unsuccessful attempts. When appropriately documented and recorded by the ISP, the explanation should provide enough information to help the adjudicator determine whether additional efforts would result in a completed scope item.

b. Relevancy of Incomplete or Missing Scope Items. It is important that an investigation include enough information to allow issue resolution. However, different scope items are relevant for different issues. In general, any case that does not include enough information to resolve the issue should be returned to the investigation provider. However, if a missing scope item is not relevant to an adjudicative issue, it may not be necessary to return the investigation, but the missing items must be documented in accordance with the August 31, 2010 USD(I) Memorandum. Adjudicators are uniquely qualified to make decisions about the relevance of sources to an issue. Guidance on adjudication of incomplete PSIs is contained in the July 13, 2010 USD(I) Memorandum.

c. Scope Item Importance. All scope items may gather information that is important to an adjudicative determination. However, some items, like a subject interview when required, are more likely to do so than others. A favorable decision made without information from these types of critical scope items generally carries a greater risk.

d. Scope Item Leads or Sources. Some investigation scope items consist of a single source of information; others may consist of multiple sources or leads. For scope items that consist of multiple sources, one missing source may not be significant enough to make it necessary to return the investigation. On the other hand, key information is missing if a single source item, such as the credit check, has not been completed.

SECTION 8: ACCESS DETERMINATIONS

8.1. ACCESS TO CLASSIFIED INFORMATION.

a. Granting national security eligibility is a function distinct from granting access to classified national security information. National security eligibility determinations are made on the merits of the individual case and involve examining a sufficient period of a person's life and background to determine that the person is an acceptable national security risk. Access determinations are made solely on the basis of the eligible individual's need for access to classified information to perform official duties.

b. The adjudication facility determines the level of eligibility based on the adjudicative record and the National Security guidelines. The employing activity determines access level based on eligibility, need-to-know, and the requirements of the position held. Before granting access to classified information, the individuals must sign the appropriate nondisclosure agreements in accordance with E.O. 12829 if JPAS does not reflect a previously signed nondisclosure agreement.

c. DoD guidance on access to classified information by individuals in the Executive Branch is contained in DoDM 5200.01. Guidance for persons outside the Executive Branch is in DoDM 5200.01.

8.2. ONE-TIME OR SHORT DURATION ACCESS. Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short-duration access to classified information at a higher level than authorized by the existing eligibility level. Requirements for one-time or short-duration access are prescribed in the December 12, 2005 Office of Management and Budget Memorandum. The exercise of this provision will be used sparingly. Repeatedly using multiple short duration accesses for the same individual during any 12-month period is prohibited.

a. Conditions. If the access granted involves another agency's classified information, then that agency must concur before access is granted. Access must not exceed 180 days and is limited to specific, identifiable information that is made the subject of a written record.

b. Procedures.

(1) Authorization will be granted by a GO/FO, a civilian equivalent, or a general court-martial convening authority after coordination with appropriate security professionals. Authorities may grant one-time or short-duration access to information classified at the same (or lower) level of access as that held by the authority.

(2) The recipient of the one-time access authorization must be a U.S. citizen and possess a current national security eligibility.

(3) Access at the next higher level for COMSEC, SCI, SAP, NATO, National Command and Control-Extremely Sensitive Information, or foreign government information is not authorized.

(4) The employee to be afforded the higher level access must have been continuously employed by a DoD Component or a cleared DoD contractor.

(5) Local, personnel, and security records of the employee concerned will be reviewed to ensure there is no derogatory information.

(6) Access at the higher level will be limited to information under the control and custody of the authorizing official and will be afforded under the general supervision of an employee cleared to the classification level for the information. The employee charged with providing such supervision is responsible for recording the higher-level information actually revealed, the date(s) such access is afforded, and the daily return of the material accessed

(7) Such access will be cancelled promptly when no longer required, at the conclusion of the authorized period of access, upon notification from the granting authority, or after 180 days from when access is granted, whichever comes first.

(8) The authorized security professional will post the one-time or short-duration access in JPAS and maintain the following for 24 months from the date the access is granted:

(a) The name and social security number of the employee afforded access.

(b) The date and level of access authorized.

(c) Compelling reason to grant the higher-level access and the benefit to the DoD mission or event.

(d) The identity of the approving authority.

c. Revocation. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight.

d. Other Circumstances. Do not use one-time or short-term access when circumstances would permit the routine processing of an individual for a higher-level security eligibility.

8.3. SPECIAL CASES. When necessary in the interests of national security, the DoD Component heads or their senior agency official may authorize access to classified information by persons outside the Federal Government, as prescribed in DoDM 5200.01.

SECTION 9: PERSONNEL SECURITY ACTIONS

9.1. GENERAL.

a. Unfavorable national security eligibility determinations do not include administrative security clearance downgrades or withdrawals based on changed duties or similar circumstances unrelated to a national security eligibility adjudication, or withdrawals of interim eligibility based on derogatory information.

b. This section provides guidance only for the internal operation of the DoD. It is not intended to, does not, and may not be relied upon to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

9.2. REFERAL OF DEROGATORY INFORMATION FOR ACTION.

a. Whenever derogatory information about an individual with national security eligibility (regardless of whether that individual has access to classified information) is developed or otherwise becomes available to any DoD element that is relevant to the adjudicative guidelines, it will be referred to the commander or the security professional of the DoD organization to which the person is assigned for duty. Reporting will be in accordance with Section7 of this manual.

b. Whenever it is determined an individual may be involved with a foreign intelligence entity, the matter will be referred to the supporting Military Department CI organization (MDCO) (for civilians or military personnel) or the FBI (for contractor personnel), with copy to DSS, as appropriate, to resolve issues related to a request for investigative or operational support. Organizations will comply with these steps unless directed to do otherwise by the MDCO or FBI:

(1) After coordinating with the supporting MDCO or the FBI, with copy to DSS, as necessary, cognizant commanders or security professionals will evaluate referred information in terms of its security significance and completeness. Commanders will coordinate with local security and law enforcement, as appropriate.

(2) Commanders or security professionals will report derogatory information and any actions taken or anticipated within 72 hours to the appropriate adjudication facility via JPAS, and make a determination on whether the derogatory information warrants the suspension of access to classified information.

(3) If further information is needed to resolve the allegations, the DoD CAF will request additional investigation. The DoD CAF will take the appropriate adjudicative action to include possible suspension of the eligibility in accordance with Paragraph 9.4.a. This does not preclude or preempt the authority of the commander or security professional with respect to the individual's local access.

c. Reports of derogatory information involving contractor personnel must be referred directly to the DSS or Personnel Security Management Office for Industry and to the DoD CAF. The DoD CAF will take the appropriate adjudicative action in accordance with Paragraph 9.5.a and referral to the DOHA for possible action, in accordance with DoDD 5220.6. Military and civilian security officers should evaluate the nature of the derogatory information and make a risk management decision whether or not to remove the individual from access pending final review by the DoD CAF or DOHA. Contractors under the NISP report in accordance with DoD 5220.22-M.

d. No final unfavorable national security eligibility determination may be taken without providing the opportunity to invoke due process protections contained in Section 7 of this manual.

9.3. LOSS OF JURISDICTION.

a. A loss of jurisdiction results when an individual retires, separates, or ends their affiliation with DoD before an adjudications facility can make an eligibility determination. Under these circumstances the adjudication facility will cease all work on the individual's adjudicative record.

b. When a loss of jurisdiction occurs the adjudication facility will register an eligibility of none in the system of record.

c. When an individual re-affiliates, the owning organization will communicate with the DoD CAF to determine whether eligibility can be established based on the existing background investigation or if a new background investigation is required.

9.4. SUSPENSION OF NATIONAL SECURITY ELIGIBILITY OR ACCESS.

a. Except for cases involving NISP contractor personnel, which are administered according to the suspension standards set by DoDD 5220.6 and Volume 2 of DoDM 5220.22, the DoD CAF and the DoD IC central adjudication facilities are solely responsible for suspending national security eligibility.

(1) The adjudication facility will evaluate any credible derogatory information it receives within 15 calendar days and make an initial determination indicating whether or not a cleared individual's continued eligibility is clearly consistent with the interests of the national security.

(2) Adjudication facility officials should confirm with the reporting organization to ensure derogatory information has been reported to CI or law enforcement authorities as appropriate.

b. DoD Component heads, commanders, or their authorized representatives, may suspend access for cause when information relative to any of the adjudicative guidelines exists and raises a serious question as to the individuals' ability or intent to protect national security information. The Director, DSS, has the authority to suspend access for cause for cleared employees of

contractors under the NISP in accordance with References DoD 5220.22-M and the May 13, 2009 USD(I) Memorandum.

c. DoD Component heads, commanders, or their authorized representatives must report access suspensions to the appropriate adjudication facility via the JPAS incident report link within the same calendar day as the suspension. This action alerts registered JPAS users of the change in the person's status. The MDCO or FBI may direct this reporting not be done.

d. DoD Component heads, heads of DoD agencies, commanders, or their authorized representatives must include a command recommendation to the supporting adjudication facility on whether to retain the individual's national security eligibility pending the conclusion of an investigation or when rendering a final determination, and provide the individual with a copy of that recommendation.

e. Local commanders or organization heads, as appropriate, must notify persons in writing when their eligibility or access has been suspended and include a brief statement of the reason(s) for the suspension of access consistent with the interests of national security.

f. Adjudication facilities must notify persons in writing when their eligibility has been suspended and include a brief statement of the reason(s) for the suspension of eligibility consistent with the interests of national security.

g. Individuals will sign a receipt, acknowledging receipt of the suspension notification, which must state that the receipt is not an acknowledgement of culpability or concurrence with the suspension.

h. The adjudication facility will render a new national security eligibility determination upon receipt of a finalized incident report associated with a suspension of national security eligibility and enter the determination in JPAS. Before restoring access, local commanders, organization heads, or security professionals must verify eligibility in JPAS.

i. Suspension cases must be resolved as quickly as circumstances permit. Suspensions exceeding 180 days must be closely monitored and managed by the adjudication facility concerned so as to expeditiously reach a new national security eligibility determination.

j. The OUSD(I&S) Security Policy and Oversight Division will monitor the number of suspensions that exceed 180 days.

SECTION 10: APPEAL PROCESS

10.1. GENERAL.

a. Individuals will be provided an opportunity to appeal an adjudication facility's unfavorable national security determination in accordance with the procedures contained in this section.

b. SCI due process procedures will be conducted in accordance with DoDI 5210.45 and Intelligence Community Policy Guidance Number 704.3, as applicable.

c. DoD Components may enter into agreements to have DOHA review written appeals and provide the Component's PSAB a recommended decision.

10.2. MINIMUM DUE PROCESS REQUIREMENTS APPLICABLE TO ALL. No unfavorable national security eligibility determination will be made without first:

a. Providing the individual with a comprehensive and detailed written explanation of the basis for the unfavorable determination as the national security interests of the United States and other applicable law permit. The LOD or LOR must include each security concern, the applicable adjudicative guideline(s) related to each concern, and provide an explanation of the kinds and types of information they could provide to support their appeal.

b. Informing the individual of their right to:

(1) Be represented by counsel or other representative at their own expense.

(2) Request the documents, records, and reports upon which the unfavorable national security determination was made. Be granted an extension to the set timeline by the Component PSAB if requested documents, records, and reports are not provided promptly.

c. Providing a reasonable opportunity to reply in writing and to request review of the unfavorable determination.

d. Providing the individual written notice of reasons for the determination, the determination of each adjudicative guideline that was provided to the individual in the statement of reasons (SOR) that accompanied the notification of intent (NOI) to deny or revoke the identity of the determination authority, and written notice of the right to appeal unfavorable determinations to a high-level panel.

e. The individual must acknowledge the receipt of the LOD or LOR and indicate in writing if they will submit an appeal. If the individual refuses to acknowledge receipt or indicate whether an appeal will be submitted, the security professional will make a written record of the refusal and submit it to the adjudication facility.

f. Providing the individual an opportunity to appear in person and present relevant witnesses, documents, materials, and information.

g. Providing the individual with a written decision on appeal.

h. When a DoD Component head or principal deputy personally certifies that a procedure in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure will not be made available. This certification is conclusive.

(1) This section does not limit or affect the responsibility and power of a DoD Component head pursuant to any law or other E.O. to deny or terminate access to classified information in the interests of national security.

(2) The power and responsibility to deny or revoke eligibility for access to classified information pursuant to any law or E.O. may be exercised only where the DoD Component head determines that the procedures prescribed in Section 7 and this section cannot be invoked in a manner that is consistent with national security. This determination is conclusive.

10.3. SPECIFIC PROCEDURES FOR CONTRACTOR EMPLOYEES.

DoD contractor personnel will be afforded the appeal procedures in DoDD 5220.6.

10.4. SPECIFIC PROCEDURES FOR CIVILIAN EMPLOYEES AND MILITARY MEMBERS.

a. No unfavorable national security eligibility determination will be rendered unless the civilian employee or military member concerned has been:

(1) Provided an LOI. The LOI to deny or revoke must accompany or include the SOR and contain:

(a) A summary of the security concerns and supporting adverse information.

(b) Instructions for responding to the SOR.

(c) A copy of the relevant adjudicative guidelines.

(d) A list and description of the information relied upon to render the proposed unfavorable national security eligibility determination.

(2) Provided a Written SOR. The SOR must state the basis for the proposed unfavorable national security eligibility determination. The SOR must be as comprehensive and detailed as national security and Section 552 of Title 5, U.S.C. and DoD 5400.11-R permit. The SOR must explain each security concern, state the specific facts that trigger each security concern, identify the applicable adjudicative guideline(s) for each concern, and provide the disqualifying conditions and mitigating conditions for each adjudicative guideline cited.

(3) Afforded an Opportunity to Reply to the LOR and SOR. The reply must be in writing to the adjudication facility.

(a) The individual must notify the adjudication facility in writing within 10 calendar days of receipt of the LOI and SOR whether he or she intends to reply to the LOI and SOR.

(b) The individual's reply to the LOI and SOR must be submitted no later than 30 calendar days from the date he or she received the LOI and SOR. An extension of up to 30 calendar days from the original deadline may be granted by the employing organization following submission of a written request from the individual before the expiration of the original deadline. Additional extensions may only be granted by the adjudication facility when factors beyond the individual's control (e.g., failure of the DoD CAF or the ISP to provide records in a timely manner) warrant granting additional time.

(c) The adjudication facilities will not deny or revoke an individual's national security eligibility without official documentation that the individual received the LOI and SOR.

(4) Provided a Written LOD or LOR.

(a) When a favorable determination cannot be rendered, the central adjudication facilities will provide the individual via the appropriate Component or command security office, a written LOD or LOR stating the final determination of each adjudicative guideline that was provided to the individual in the statement or reasons (SOR) that accompanied the NOI to deny or revoke was mitigated or unmitigated and reason(s) for denying or revoking national security eligibility.

(b) The LOD or LOR will include clear instructions on how to appeal the unfavorable determination.

(c) The central adjudication facilities will provide the written LOD or LOR as promptly as individual circumstances permit but no more than 60 calendar days from the date of receipt of the individual's reply to the SOR and LOI, provided no additional information is deemed necessary to render the national security eligibility determination.

(d) When an LOD or LOR is based on the failure of the individual to reply to the SOR and LOI, the LOD or LOR will include all of the security concerns, adjudicative guidelines, and mitigating factors contained in the SOR and LOI and the reason(s) for denying or revoking national security eligibility.

(e) If an LOD or LOR cannot be completed within the time frame allowed, the individual will be notified in writing of this fact, the reasons why, and the date the written LOD or LOR is expected to be completed, which will not normally exceed a total of 90 calendar days from the date of receipt of the reply to the SOR and LOI.

(f) The DoD Component or command security professionals will notify the appropriate adjudication facility within 10 calendar days if they are unable to deliver the LOD or LOR to the individual. The notification will include information as to why the LOD or LOR could not be delivered (e.g., illness or death in the family, deployment) and when it is expected

the individual can receive a copy of the LOD. Security professionals must deliver the LOD immediately upon the individual's return.

(5) Afforded an Opportunity to Appeal the LOD or LOR.

(a) Within 10 calendar days of receipt of LOD or LOR, the individual will sign and return the notice of intent to appeal (NOIA) to the adjudication facility via their security office. The individual must state whether he or she intends to appeal, and if so, whether he or she requests a personal appearance or will appeal in writing. The local security professionals may grant a single 10 calendar day extension upon request from the individual. The grant of a 10 calendar day extension must be annotated in JPAS. All other requests for extension must be granted by the adjudication facility.

(b) Within 4 calendar days of receipt of the individual's NOIA, security offices will forward the NOIA to the adjudication facility.

(c) The adjudication facility will store signed statements acknowledging receipt of LOD and NOIA electronically in the subject's adjudicative record.

(d) If the individual elects to appeal the LOD or LOR, the adjudication facility will forward a copy of the NOIA within 2 calendar days to the appropriate PSAB and to DOHA if a personal appearance is requested. The adjudication facility will also forward the individual's adjudicative record within 2 calendar days to the appropriate PSAB for direct appeals or to DOHA if a personal appearance is requested. The adjudicative record will contain all of the materials the adjudication facility relied upon to render its determination as well as the LOI, SOR, LOD or LOR, the commander's recommendation, and any rebuttal materials the individual provided in response to the LOI/SOR.

(e) If a decision is made to appeal the LOD or LOR, individuals may do so by:

1. Written appeal directly to the applicable DoD Component PSAB. Individuals must, within 30 calendar days of receipt of a LOD or LOR, write to the applicable DoD Component PSAB stating reasons why the denial or revocation should be overturned and provide any additional relevant information that may have a bearing on the case. The appeal and supporting documentation will be transmitted to the DoD Component PSAB via the individual's security office. The DoD Component PSAB president or designee may grant a 30 calendar day extension of time for good cause demonstrated by the appellants (e.g., illness or death in the family, deployment).

2. Appendix 7B to this manual explains the personal appearance process before a DOHA AJ.

(6) Provided a Final Written Decision by the DoD Component PSAB. The DoD Component PSAB will review the adjudicative file and any appeal materials (including the DOHA AJ recommendation, if applicable), and render a final decision. If the DoD Component PSAB agrees with the AJ's written recommendation, the DoD Component PSAB may adopt the AJ's written recommendation in lieu of providing a DoD Component PSAB written determination. The individual will be notified of the DoD Component PSAB's final

determination via the subject's security professional, generally within 45 calendar days of the receipt of a direct appeal or 30 calendar days from receipt of the AJ recommendation. The DoD Component PSAB's written decision will identify each adjudicative guideline issue stated in the LOD or LOR that formed the basis of the denial or revocation that remains unmitigated after the appeal and the rationale for the final disposition of the appeal.

(7) New Information Considered by the DoD Component PSAB. Should the president of the DoD Component PSAB determine that information not contained in the adjudicative record or the appeal material is needed to render a final determination (e.g., updated credit bureau report, information from the command) such information must be provided to the individual, who then must be provided a reasonable period of time to offer any rebuttal to this information, before it being considered by the DoD Component PSAB.

b. The head of the local organization of the individual receiving a SOR and LOI will designate a POC to serve as a liaison between the adjudication facility and the individual. The duties of the POC will include, but are not limited to:

(1) Delivering the SOR and LOI and having the individual acknowledge receipt of the SOR and LOI. POCs and a witness will document the delivery if the individual refuses acknowledgement.

(2) Determining whether the individual intends to respond within the time specified and reporting this information to the adjudication facility.

(3) Explaining the consequences of the proposed action and the need to respond in a timely fashion.

(4) Explaining how to obtain time extensions.

(5) Explaining how to obtain copies of investigative records.

(6) Explaining the procedures for responding to the SORs.

(7) Explaining individuals' entitlement to obtain legal counsel or other assistance at their own expense within the relevant time periods.

10.5. RECORDING FINAL DETERMINATINOS. DoD Component PSABs will provide electronic copies of all final decisions to the adjudication facility that made the initial unfavorable determination. The adjudication facility will update JPAS within 2 calendar days to reflect current eligibility and append the DoD Component PSAB decision to the individuals' adjudicative records.

10.6. RECONSIDERATION. Commanders may request reconsideration of unfavorable national security determinations for individuals within their command to address specific mission needs after the passage of 1 year following a denial or revocation. The year is counted from the date of the denial or revocation decision by the consolidated adjudication facility; or, if

the individual elected to appeal, 1 year from the date of the final appeal determination. Individuals who terminate their affiliation with DoD for 24 months or more after a unfavorable national security determination are not subject to the reconsideration process. When attempting to re-affiliate with DoD these individuals will be submitted for a new investigation.

a. DoD Components' requests for reconsideration will be examined only when forwarded and recommended by officials of the employing Component.

b. Not all cases meet the test for reconsideration, and passage of time alone is not a sufficient criterion. Occasionally, the issues in a case will be so recent or serious that a longer time may be appropriate to resolve the issues or to establish an affirmative track record to minimize the probability of recurrence.

c. If a denial or revocation is based on significant derogatory information that has been reported to a CI or law enforcement authority, the DoD CAF should consult with the CI or law enforcement authority before reconsideration to ensure it has all relevant information.

d. The requirements for DoD Component requests for reconsideration are:

(1) The individual's eligibility has been denied or revoked for at least 1 year. The year is counted from the date of the denial or revocation decision by the adjudication facility, or, if the individual elected to appeal, 1 year from the date of the final appeal determination.

(a) When 2 years or more have passed, the DoD Component will determine what checks or investigations are required to support the reconsideration.

(b) A new national security investigation must be conducted by the ISP and the report of investigation adjudicated to determine if eligibility will be granted when there has been a 2-year break in service or the last investigation is out of scope.

(2) Cases will not be resubmitted or reassessed solely based on an individual's personal desire to acquire eligibility. Reconsideration is not a personal right or entitlement.

(3) DoD Component requests for reconsideration must be made to the adjudication facility from security office(s) and must meet an operational need of the DoD Component. The individual must be selected or tentatively selected for a national security position. Requests for reconsideration will include explicit statements of DoD Component support.

(4) Security offices will ensure DoD Component requests for reconsideration are complete. The request must include evidence that the issues which caused the denial or revocation have been resolved.

(5) Once security offices submit their DoD Components' request for reconsideration, no supplemental information will be accepted or considered unless requested by the adjudication facility. Information requested by the adjudication facility will be submitted within the time specified by the adjudication facility.

(6) A DoD Component's request for reconsideration does not reopen or otherwise affect the denial or revocation decision.

e. Commands seeking reconsideration are responsible for providing documentation that the circumstances or conditions that resulted in the final adverse eligibility determination have been rectified or sufficiently mitigated to warrant reconsideration, which will be forwarded to the adjudication facility by the DoD Component.

f. The adjudication facility has the authority to grant or deny the reconsideration based on a review of the DoD Component documentation to determine the extent to which circumstances or conditions have been rectified or sufficiently mitigated.

g. When a reconsideration determination is denied, the adjudication facility will provide notification through the command to the DoD Component in writing, generally within 30 days from receipt of request for reconsideration.

h. JPAS will be annotated accordingly.

i. No due process is afforded for denial of a DoD Component's request for reconsideration.

j. Commands may determine the submission of a new background investigation is merited rather than a request for reconsideration.

k. For reconsideration cases involving NISP contractor personnel, see DoDD 5220.6.

10.7. REINSTATEMENT OF CIVILIAN EMPLOYEES. A DoD civilian whose employment was terminated based on the denial or revocation of national security eligibility will not be reinstated, restored to duty, or reemployed in a sensitive or national security position in the DoD unless the Secretary of Defense or the employee's DoD Component head finds that doing so is clearly consistent with the interests of national security. That finding must be made part of the personnel security record.

APPENDIX 10A: PSAB STRUCTURE AND FUNCTIONING

PSAB panels will be structured and function to meet these requirements:

a. The PSAB will include a president and two members.

(1) The PSAB president will be a DoD military member or civilian at a minimum grade of O-6 or general schedule/general grade-15 or equivalent. There will be no more than one security specialist on the PSAB.

(2) Board members will be of a minimum grade of O-5 or general schedule / general grade-14 or equivalent.

(3) At least one board member will be equivalent or senior in grade to the appellant.

(4) One board member may be an attorney, unless the board has access to legal counsel.

(5) Officials from the adjudication facility will not serve as a member of the PSAB.

b. The PSAB will:

(1) Process appeals in a first in, first out basis.

(2) Process appeals with appearances before DOHA within 30 calendar days of receipt of the recommendation of the AJ.

(3) Process direct appeals within 45 calendar days of receipt.

(4) Require each board member review each appeal received independently and conduct a de novo review of each of the unmitigated adjudicative guideline issues that were stated in the LOD or LOR.

(5) Not communicate with officials from the adjudication facility concerning case merits. However, in cases where the PSAB identifies relevant information that was available during the DoD CAF adjudication process but was not considered by the DoD CAF, the PSAB president may remand the case back to the DoD CAF and request appropriate action.

(6) Require all board members to participate in the discussion of the merits of each appeal and cast an independent vote on whether to affirm or overturn the unmitigated adjudicative guideline issues stated in the LOD or LOR. Appeals will be decided by majority vote.

(7) Conclude the appeal process with issuing the majority PSAB determination which will be final.

(8) Notify appellants in writing of the PSAB's final determination and supporting rationale through command channels.

APPENDIX 10B: PERSONAL APPEARANCES BEFORE DOHA

10B.1. The adjudication facility will provide DOHA with a copy of appeal through personal appearance NOIAs and the individual's adjudicative record within 2 calendar days of receipt of the NOIA via the CATS portal.

10B.2. The DOHA will assign the case to an AJ within 2 work days of receipt of the NOIA.

10B.3. The AJ will schedule a personal appearance (generally within 30 calendar days from receipt of the request), and arrange for the production of a verbatim transcript of the proceedings.

10B.4. For appellants at duty stations within the contiguous United States, personal appearances may be conducted at a DOHA site, at an appellant's duty station, a nearby suitable location, or via video teleconference (VTC). For individuals assigned to duty stations outside the 48 contiguous states, personal appearances generally will be conducted via VTC using a suitable location at or near the appellant's duty station.

10B.5. Any travel costs for appellants to appear in person at a DOHA location or at a duty station near their location will be the responsibility of the employing organization, if the employer cannot provide means for VTC from the appellant's location.

10B.6. AJs will conduct proceedings in a fair and orderly manner.

10B.7. Appellants may:

a. Be represented by counsel or personal representative at their own expense.

b. Make oral presentations, and respond to questions posed by counsel or personal representative. Appellants must also respond to questions asked by the AJs or DOHA counsel.

10B.8. The appellant and DOHA counsel may:

a. Submit documents relative to whether the LOD or LOR should be overturned.

b. Present or cross-examine witnesses.

10B.9. Witnesses will appear at no cost to the government.

10B.10. Witnesses may address matters relevant to the establishment, refutation, extenuation, or mitigation of the facts alleged in the SOR.

10B.11. Neither appellants nor the AJs may challenge the official U.S. Government characterization of the nature of any country, organization, or individual other than the individual or the individual's witnesses.

10B.12. The DOHA AJ will conduct a de novo review of the unmitigated adjudicative guideline issues stated in the LOD or LOR and issue, generally within 30 calendar days of the close of the record, written recommendations to the appropriate PSAB whether to sustain or overturn the denial or revocation. DOHA's recommendations will set forth pertinent findings of fact, policies, and conclusions as to the unmitigated adjudicative guideline issues stated in the LOD or LOR and whether it is clearly consistent with the national security interests of the United States to grant or deny the appellant's national security eligibility. DOHA's recommendation along with the adjudicative file and any documents submitted by the appellant will be forwarded to the appropriate PSAB via the CATS portal.

10B.13. DOHA will provide the DoD Component PSAB with a weekly status update for all cases that exceed 30 calendar days. The update will include the name of the appellant, the case number, the date of the personal appearance hearing, the date the record will close, and the projected date the AJ recommendation will be finalized.

SECTION 11: CE AND REPORTING REQUIREMENTS

11.1. GENERAL.

a. Personnel security determinations assess whether an individual can be trusted to protect national security. It is impossible to establish with certainty, based on an eligibility determination that human beings will continue to behave in ways to retain such trust. Accordingly, a favorable national security eligibility determination is but one facet of an effective personnel security program.

b. CE is the periodic reviewing of the individual's background to determine whether they continue to meet the requirements for national security eligibility. DoDI 5200.02 requires all personnel in national security positions will be subject to CE.

c. DoD Components must continuously assess those employees with favorable national security determinations to ensure they can continue to be trusted to protect national security. Organizational commanders or managers, supervisors, co-workers, and individuals with favorable national security eligibility determinations have a personal responsibility to expeditiously report behaviors they observe or commit that cause a security concern, such as:

(1) Any incident or behavior identified in the August 30, 2006 USD(I) Memorandum; Intelligence Community Policy Guidance Number 704.1; and Volume 2 of DoDM 5220.22 will be reported first to the supervisor, security professional, or commander. This includes, but is not limited to, reporting of investigations of government travel card misuse, abuse, or fraud.

(2) A crime will be reported to a law enforcement authority.

(3) An incident or behavior will be reported to the MDCO in accordance with DoDD 5240.06.

(4) Information that suggests an individual may have an emotional, mental, or personality condition that can impair judgment, reliability, or trustworthiness will be reported to the supporting adjudication facility. Such information may include, but is not limited to:

(a) A known history of a mental disorder.

(b) A report that an individual has sought treatment for a mental, emotional, or substance abuse condition (commensurate with any reporting limitations of Section 21 on the SF86).

(c) Direct and indirect threats of violence.

(d) Physical altercations, assaults, or significant destruction of U.S. Government property.

(e) An abrupt and significant change in an individual's appearance or behavior suggesting impaired judgment or stability (e.g., deteriorating physical appearance or self-care, social withdrawal).

(f) Signs of substance use or intoxication on the job.

(g) An indication of substance abuse after completion of treatment.

(h) Evidence of alcohol or drug related behavior outside the workplace (e.g., driving under the influence, public intoxication charges).

(i) Suicide threats, attempts, or gestures or actions.

(j) Any other behaviors which appear to be abnormal and indicate impaired judgment, reliability, or maturity.

d. Reporting requirements for contractors are established in DoD 5220.22-M.

11.2. CE RESPONSIBILITIES.

a. Commanders, DoD Component Heads, Directors, Supervisors, and Security Professionals' Responsibilities. Supervisors, managers, and security professionals play a critical role in assuring the success of the CE program. The goal of CE is timely detection and reporting of potential issue information.

(1) Commanders, DoD Component heads, and directors of organizations will ensure that:

(a) Personnel assigned to sensitive duties receive initial security briefing and annual refresher briefings on the national security implications of their duties and their individual responsibilities. These briefings will emphasize the individuals' responsibility to meet the standards and criteria for security eligibility as stated in the December 29, 2005 White House Memorandum and Intelligence Community Policy Guidance 704.2.

(b) Personnel in national security or sensitive positions are provided with information about available programs (e.g., employee assistance) designed to help employees address questions or concerns regarding issues that may affect their ability to remain eligible for access to classified or assignment to sensitive positions.

(c) Unfavorable information (e.g. government travel card misuse, abuse, or fraud and administrative or disciplinary action taken as a result of management review or investigation) is reported to the appropriate security, law enforcement, or CI professionals for appropriate action. Upon coordination with CI and law enforcement professionals as necessary, unless directed otherwise by the supporting CI professional, the incident report will be forwarded to the adjudication facility via JPAS. Local commanders may suspend access to classified information or assignment to sensitive duties if they believe the behavior causes doubts about whether the individual's continued access is in the best interest of national security. Access to classified information or assignment to sensitive duties may be restored following the supporting

adjudication facility's favorable national security determination. However, if issues have not been resolved within 20 calendar days, action must be taken in accordance with Section 3 of this manual. When the unfavorable information relates to a contractor employee, the USD(I&S) and the Director, DSS have the authority to take interim suspension action in accordance with DoDD 5220.6, Volume 2 of DoDM 5220.22, and the May 13, 2009 USD(I) Memorandum.

(d) Supervisory personnel are informed of their personnel security responsibilities and provided guidance on indications of potential personnel security concerns and procedures to follow to report them in a timely manner. Programs will include:

1. Training and continuous education on reportable behaviors.

2. Procedures for immediate reporting of derogatory information (e.g. government travel card misuse, abuse, or fraud and associated investigations and administrative or disciplinary action taken) through appropriate channels to the appropriate adjudication facility.

3. Outreach to inform personnel of programs to address behavior(s) that may affect their continued eligibility for access to classified information or assignment to a sensitive position.

(e) Reporting by health care professionals regarding military personnel is subject to the limitation required by DoDI 6490.08.

(2) Supervisors will:

(a) Continuously evaluate individuals with national security eligibility to determine if they continue to be trustworthy in accordance with the security standards in the adjudicative guidelines enumerated in the December 29, 2005 White House Memorandum and Intelligence Community Policy Guidance 704.2, or successor documents, as appropriate.

(b) Report any derogatory information that falls within the adjudicative guidelines (e.g. government travel card misuse, abuse or fraud) to their cognizant security professional or commander. Failure to report derogatory information may trigger an adverse security action in accordance with Paragraph 11.2.b.

(c) Ensure the discharge of security responsibilities is included in personnel performance evaluations, pursuant to Section 552a of Title 5, U.S.C. and in accordance with applicable DoD Component guidance.

(3) Security professionals, at the direction of the commander, will:

(a) Report unfavorable information meeting the reportable behavior guidelines contained in the Appendix 5A to the supporting adjudication facility, law enforcement, or CI supporting activity. When authorized, forward the report to the adjudication facility via JPAS or the CATS Portal, as appropriate.

(b) Provide the following details for all security incidents or issues of a security concern (to the extent available):

1. Nature and seriousness of the conduct.

2. Circumstances surrounding the conduct.

3. The frequency and recency of the conduct.

4. The age of the individual at the time of the conduct.

5. The voluntariness or willfulness of the individual's participation or conduct.

6. The knowledge the individual had of the consequences involved.

7. The motivation for the conduct.

8. How the command became aware of the information.

9. Actions the individual has taken to correct the issue, including medical treatment, counseling, lifestyle changes, or other corrective actions.

10. The stability of the individual's lifestyle or work performance, including demonstrative examples.

11. Cooperation on the part of the individual in following medical or legal advice or assisting in command efforts to resolve the security issue.

12. A command recommendation to the supporting adjudication facility with a copy of that recommendation to the individual on whether to retain an individual's eligibility pending the conclusion of a national security investigation or when rendering a final determination.

(c) Report unfavorable information that becomes available concerning cleared NISP contractor personnel to the DoD CAF, DSS, and to the contractor facility security officer.

b. Employee Responsibilities. All employees are obligated to advise the appropriate authorities or officials when they become aware of any information, behavior, or conditions that may pose a security concern, or that raise doubts whether a co-worker's eligibility or access to classified information or assignment to sensitive duties is consistent with national security. If it is proven that an employee failed to report facts about a co-worker, an adverse national security eligibility action may be initiated against the employee who failed to report it.

c. Individual Responsibilities. Personnel should familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, they should be aware of the standards of conduct required of persons with national security eligibility as well as the security requirements of those positions. They should recognize and avoid the kind of personal behavior (i.e. government travel card misuse, abuse, or fraud) that would render them ineligible for continued access to classified information or assignment to sensitive positions. In the final analysis, the ultimate responsibility for maintaining continued national security eligibility rests with the individuals. Personnel having access to classified information will:

(1) Protect classified information in their custody from unauthorized disclosure.

(2) Be aware of and comply with PR, CE, and reporting requirements.

11.3. ADDITIONAL REPORTING REQUIREMENTS FOR INDIVIDUALS WITH ACCESS TO SCI INFORMATION. Individuals with access to SCI information will comply with reporting requirements identified in Volume 3 of DoDM 5105.21.

11.4. FINANCIAL DISCLOSURE. Individuals who have been identified by their respective DoD Component head must file with their respective DoD Component a financial disclosure report in accordance with Section 1.3(a) of E.O. 12968.

a. Financial disclosure information will be reported using SF 714, "Financial Disclosure Report," or an equivalent form approved by the SecEA.

b. Failure to submit required financial information may result in the withdrawal of access to classified information.

11.5. POST-ADJUDICATION ISSUES. Upon receipt of a report of adverse information from any source, an adjudicator will evaluate the report and determine whether post-adjudicative actions are required. If the adjudicator's review determines the reported information is not adequate or detailed enough to make an eligibility determination, the adjudicator may employ authorized means (e.g., requests for special investigations, interrogatories, contacts with subjects and employers, requests for information from security professionals, requests for medical or psychological evaluation, and record searches) to obtain additional information to make an eligibility determination.

SECTION 12: EDUCATION, TRAINING, AND PROFESSIONAL CERTIFICATION

12.1. EDUCATION AND TRAINING REQUIREMENTS.

a. General. Training on security responsibilities is an integral part of the DoD PSP and is essential to its efficient functioning.

b. Education and Training Programs.

(1) Security education and training programs are required for DoD security professionals and other personnel performing security duties on the procedures necessary to protect information and on the personnel security process. Training topics include: JPAS and e-QIP, orientation, indoctrination, initial briefings, refresher briefings, debriefings, termination briefings, travel briefings, foreign contact briefings, and intelligence threat briefings.

(2) For assistance in meeting security education and training program requirements, visit the DSS Center for Development of Security Excellence (CDSE) website at http://www.cdse.edu. The CDSE website includes personnel security courses, job aids, reference guides, and webinars addressing the security clearance process, JPAS, e-QIP, and various "security shorts."

c. Initial Briefing. All personnel with national security eligibility will be given an initial security briefing that is compliant with the requirements of E.O. 12968; Volume 3 of DoDM 5200.01; and the February 9, 1999 Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence Memorandum, before gaining access to classified information. All individuals will execute the appropriate nondisclosure forms in accordance with Section 552 of Title 5, U.S.C. If individuals decline to execute the nondisclosure forms, the DoD Component will withhold classified access and report the refusal to the adjudication facility. DoD Components will maintain records of all initial briefings.

d. Refresher Briefing. Personnel with national security eligibility will receive annual refresher security training in accordance with DoDM 5200.01. Security education should be on a continuing basis, taking into account each person's duties, experience, and past conduct involving the protection of classified or sensitive information. DoD Components will maintain records of all refresher training conducted.

e. Insider Threat Briefing. Insider threat awareness will be incorporated into security training in accordance with DoDD 5240.06 and DoDI 5240.26.

f. Termination Briefing.

(1) Service members, federal civilian employees, and contract employees will be given a termination briefing in accordance with DoDM 5200.01 upon termination of employment, withdrawal of national security eligibility, or other absence that excludes an individual from CE authorizations and will complete a security termination statement or, for SCI access, the Security

Debriefing Acknowledgement and Debrief blocks on the reverse of DD Form 4414, "Sensitive Compartmented Information Nondisclosure Agreement" found at http://www.dtic.mil/whs/directives/forms/index.htm.

(2) When an individual refuses to execute a General Services Administration Form 3162, "Security Termination Statement," every effort will be made to debrief the individual orally. Report the refusal to sign immediately to the security professional of the cognizant organization, to the supporting adjudication facility, and record in JPAS.

(3) When individuals are unable to execute a Security Termination Statement (e.g., death, incapacitation, could not be located), make a notation reflecting the individual's status on the Security Termination Statement, report to the supporting adjudication facility, and record in JPAS.

12.2. APC PROGRAM.

a. The DoD objective is to ensure all DoD personnel security adjudicators are trained, fully qualified, and certified to perform their critical duties as prescribed in the January 28, 2014USD(I) Memorandum.

b. The APC Program will certify DoD and DoD IC personnel security adjudicators have demonstrated mastery of essential adjudicative competencies related to determining the national security eligibility of a government employee, Service member, defense contractor employee, or other affiliated person.

c. Adjudicators will be certified to perform all adjudicative functions except due process determinations, as detailed in Section7 of this manual. If adjudicators are required to make due process determinations, an additional due process credential is required before performing the function.

d. DoD CAF and DoD IC central adjudication facilities directors experiencing a critical shortage of certified adjudicators may request approval of a risk management plan for non-certified adjudicators to perform final adjudications before certification, pursuant to requirements contained in the April 10, 2009 USD(I) Memorandum. The risk management plan must be endorsed by the adjudication facility Component head and approved by OUSD(I&S) Security Policy and Oversight Director before implementation.

e. Information on the APC governance, organization, eligibility, and requirements for certification maintenance may be reviewed at the DSS CDSE website, available at http://www.cdse.edu/.

GLOSSARY

G.1. ACRONYMS.

AJ	administrative judge
ANACI	Access National Agency Check and Inquiries
APC	Adjudicator Professional Certification
CATS	Case Adjudication Tracking System
CDSE	Center for Development of Security Excellence
CE	continuous evaluation
CI	counterintelligence
CMO	Chief Management Officer of the Department of Defense
COMSEC	communications security
CSA	cognizant security agency
DDI(I&S)	Director of Defense Intelligence for Intelligence and Security
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DNI	Director of National Intelligence
DoD CAF	DoD Consolidated Adjudications Facility
DoDD	DoD directive
DoDHRA	DoD Human Resources Activity
DoDI	DoD instruction
DoDM	DoD manual
DOE	Department of Energy
DOHA	Defense Office of Hearings and Appeals
DOS	Department of State
DSS	Defense Security Service
E.O.	Executive order
e-adjudication	electronic adjudication
e-application	electronic application
e-QIP	electronic questionnaire for investigations processing
FBI	Federal Bureau of Investigation
FIS	Federal Investigative Standards
GO/FO	general or flag officer
GC DoD	General Counsel Department of Defense

IC	Intelligence Community
ISP	investigative service provider
JPAS	Joint Personnel Adjudication System
LAA	limited access authorization
LOD	letter of denial
LOI	letter of intent
LOR	letter of revocation
MDCO	Military Department CI organizations
NACLC	National Agency Check with Law and Credit
NATO	North Atlantic Treaty Organization
NGA	National Geospatial-Intelligence Agency
NISP	National Industrial Security Program
NOIA	notice of intent to appeal
NRO	National Reconnaissance Office
OPM	U.S. Office of Personnel Management
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
POC	point of contact
PPR	phased periodic reinvestigation
PR	periodic reinvestigation
PSAB	Personnel Security Appeal Board
PSI	personnel security investigation
PSP	personnel security program
RD	restricted data
SAP	special access program
SCI	sensitive compartmented information
SecEA	Security Executive Agent
SF	standard form
SOI	security office indicator
SON	submitting office number
SOR	statement of reasons
SORN	system of record notice
SPēD	Security Professional Education Development Program

SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation – Periodic Reinvestigation
TS	Top Secret
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Service
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USO	United Service Organizations
VTC	video teleconference
WHS	Washington Headquarters Services
WWSIIP	Wounded Warrior Security and Intelligence Internship Program

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

access. The ability and opportunity to obtain knowledge of national security information. An individual may have access to national security information by being in a place where such information is kept, if the security measures that are in force do not prevent the individual from gaining knowledge of such information.

adjudication. Defined in E.O. 13467.

adjudicative guidelines. Guidelines established for determining eligibility for access to classified information.

adjudicator authority. Adjudicators with the authority to grant, suspend, deny, or revoke SCI eligibility concurrently grant, suspend, deny, or revoke associated collateral eligibility unless the collateral is held by the individual's own organization. Adjudicators with the authority to grant, suspend, deny, or revoke TS eligibility concurrently grant, suspend, deny, or revoke Secret and Confidential eligibility.

adjudication facility. A facility with assigned adjudicators certified to evaluate PSIs and other relevant information to determine if granting or continuing national security eligibility is clearly consistent with the interests of national security. The DoD consolidated adjudications facility is known as the DoD CAF.

agency. Defined in DoDM 5200.22.

calendar day. Monday through Sunday.

CATS. The DoD system of record for non-IC agencies case management and adjudications.

CE. Defined in DoDM 5200.22.

CI. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

classified information. Defined in E.O. 13467 .

cohabitant. A person with whom an individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom an individual resides for reasons for convenience (e.g., a roommate).

collateral eligibility. TS, Secret, or Confidential levels of eligibility.

commander. Heads of DoD Components, Defense Agencies, DoD Field Activities, and all other entities within the DoD headed by personnel specifically assigned to command positions within organizations.

conclusive. Serving to settle or decide a question; decisive; convincing. The decision cannot be appealed to a higher authority.

condition. See "exception."

contractor. Defined in E.O. 13467.

controlled substance. Any drug, material, or other chemical compound identified and listed in DNI Memorandum ES 2014-00674.

controlled unclassified information. Defined in DoDM 5200.01.

current. An investigation that is no more than 5 years old. If JPAS reflects an open investigation, or a pending adjudication not more than 1 year beyond the 5 year anniversary date, the investigation is considered current.

CSA. Defined in DoD 5220.22-M.

damage to the national security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information, or other breach of security responsibilities by personnel serving in national security positions.

derogatory information. Information that reflects on the integrity or character of an individual, or circumstances that suggests that their ability to safeguard national security information may be impaired, that their access to classified or sensitive information clearly may not be in the best

interest of national security, or that their activity may be in conflict with the personnel security standards or adjudicative guidelines.

deviation. See "exception."

due process. An established administrative process designed to ensure the fair and impartial adjudication of facts and circumstances when an unfavorable national security eligibility determination is being considered. The process is offered to individuals before a final unfavorable determination of national security eligibility is made.

eligibility determination. The decision to grant eligibility for access to classified information or performance of national security duties.

employee. Defined in E.O. 12968.

e-adjudication. Automated adjudication, also referred to as electronic adjudication.

e-application. A web-based tool for self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct investigations. The e-QIP is the current e-application used within DoD.

e-QIP. A secure web-based automated system that facilitates timely and accurate processing of investigation requests to OPM. Agencies authorize applicants to access the system to enter data and documents required for the investigation; the system collects information from the applicant based on the appropriate investigative questionnaire.

exception. An adjudicative decision to grant or continue access eligibility despite a failure to meet adjudicative or investigative standards. For purposes of reciprocity, the presence of an exception permits the gaining organization or program to review the case before assuming security sponsorship and to accept or decline sponsorship based on that review. When accepting sponsorship, the gaining organization or program will ensure that the exception remains a matter of record. There are three types of exceptions:

condition. Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access, and restrictions on an individual's handling of classified information.

deviation. Access eligibility granted or continued despite a significant gap in coverage or scope in the supporting background investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of 6 months or more within the most recent 5 years investigated or the lack of an FBI name check or an FBI fingerprint check or the lack of one or more investigative scope requirements in its entirety (e.g., the total absence of local agencies checks within an investigation would constitute a deviation, but the absence of local agencies checks for some but not all places of residence would not constitute a deviation).

waiver. Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. "Substantial issue information" for this purpose means information in the individual's history that does not meet the standards of

national security adjudicative guidelines in the August 30, 2006 USD(I) Memorandum. DoD Component heads may approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring, and other restrictions beyond normal need-to-know on the person's handling of classified information.

exceptionally grave damage. The capacity to cause extremely serious harm.

foreign intelligence entity. Defined in DoDD 5240.06.

foreign national. Defined in the DoD Dictionary of Military and Associated Terms.

IC. Defined in the DoD Dictionary of Military and Associated Terms.

illegal drug. "A controlled substance included in Schedule I or II, as defined by Section 802(6) of E.O. 12564.

inestimable damage. The capacity for harm too severe to be computed or measured.

inherently governmental. Defined in the Federal Acquisition Regulation.

investigative record. The official record of all data obtained on the individual from trusted ISPs, from suitability or security applications and questionnaires, and any investigative activity conducted in accordance with the December 13, 2008 DNI and OPM Memorandum.

Investigation Service Provider (ISP). A federal agency or federal contract agency that conducts PSIs for the DoD.

issue information. Any information that could adversely affect a person's national security eligibility.

JPAS. The DoD system of record for personnel security adjudication, clearance, verification, and history. The term applies not only to this system but to any successor DoD personnel security system of record. JPAS has two applications. The Joint Adjudication Management System and the Joint Clearance and Access Verification System. Joint Adjudication Management System is the application that supports central adjudication facilities personnel and provides capabilities and data such as case management and distribution, adjudication history, due process history, revocations and denial action information. Joint Clearance and Access Verification System is the application that supports command security personnel and provides capabilities and data such as local access record capabilities, debriefings, incident file reports and eligibility data, and security management reports.

LAA. Authorization for access to confidential or secret information granted to non-U.S. citizens and immigrant aliens, limited to only that information determined releasable by a U.S. Government designated disclosure authority to the country of which the individual is a citizen, in accordance with DoDD 5230.11. Access is necessary for the performance of the individual's assigned duties with the military or a federal agency and is based on favorable adjudication of a 10-year scope SSBI or its equivalent under the FIS.

MDCO. Defined in DoDD 5240.06.

mentally incompetent. An individual who has been declared mentally incompetent as determined by competency proceedings conducted in a court or administrative agency with proper jurisdiction.

meritorious waiver. A determination made by authorized adjudicators that an individual meeting the criteria of the Bond Amendment has sufficiently explained, refuted, or mitigated the potential disqualifiers as to be deemed eligible for access to classified information.

national security. The national defense or foreign relations of the United States. National security includes defense against transnational terrorism.

national security duties. Duties performed by individuals working for or, on behalf of, the Federal Government that are concerned with the protection of the United States from foreign aggression or espionage, including development of defense plans or policies, intelligence or CI activities, and related activities concerned with the preservation of the military strength of the United States, including duties that require eligibility for access to classified information in accordance with E.O. 12968 .

national security eligibility. The status that results from a formal determination by an adjudication facility that a person meets the personnel security requirements for access to classified information or to occupy a national security position or one requiring the performance of national security duties.

national security information. Information that has been determined, pursuant to E.O. 13526, to require protection against unauthorized disclosure and is so marked when in documentary form.

national security position. Defined in DoDI 5200.02.

need to know. A determination made by a possessor of classified information that a prospective recipient, in the interest of the national security, has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge of, possession of, or access to, classified information will not be afforded to any individual solely by virtue of the individual's office, position, or security eligibility.

NISP. The program established by DoDM 5200.01 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government as the single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests, as governed by U.S. Office of Personnel Management Booklet and E.O. 10865.

personnel security. Defined in the June 13, 2013 Deputy Under Secretary of Defense for Intelligence and Security Memorandum.

position designation. The assessment of the potential for adverse impact on the integrity and efficiency of the service, and the degree to which, by the nature of the civilian position, the occupant could bring about a material adverse effect on the national security.

PPR. A periodic reinvestigation which excludes select investigative leads when no information of security concern is developed by the required investigative source as prescribed in the Office of Personnel Management Federal Investigative notice No. 05-04. A periodic reinvestigation conducted in phases, in which the key investigative elements yielding the greatest amounts of issue information are conducted first. The second phase of the investigation is run only if issue information results from the first phase.

PR. A national security investigation conducted to update a previously completed investigation on persons holding a national security position or performing national security duties to determine whether that individual continues to meet national security requirements.

PSAB. A three-member panel of senior level personnel authorized to make final national security eligibility determinations that have been appealed by subjects of national security investigations.

PSI. Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD for access to classified information, acceptance or retention in the Military Departments, assignment or retention in sensitive duties, or other designated duties requiring such investigation. It also includes investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for a national security position.

public trust. Defined in Federal Investigative Standards.

referral. Notification of commanders, security officers, and CAFs when relevant, and material derogatory information concerning an individual who has been granted national security eligibility is developed or otherwise becomes available to any DoD element.

reportable behavior. Acts by persons with favorable national security eligibility determinations that may not be consistent with the interests of national security.

SAP. Defined in the DoD Dictionary of Military and Associated Terms.

SCI. Classified information concerning or derived from intelligence sources, methods, or analytical process that is required to be handled within a formal access control system established by the DNI.

scope. The time period to be covered and the sources of information to be contacted during the prescribed course of a national security investigation.

SecEA. The DNI is the U.S. Government national authority responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of national security investigations and adjudications relating to determinations of eligibility for

access to classified information or eligibility to hold a sensitive position, as well as other security duties as delineated in E.O. 13467.

security clearance. A personnel security determination by competent authority that an individual is eligible for access to national security information, under the standards of this manual. Also called a clearance. The individual must have both eligibility and access to have a security clearance. Eligibility is granted by the central adjudication facilities, and the access is granted by the individual agencies.

security incident. Defined in Title 50, U.S.C.

security professional. U.S. Government military or civilian personnel (including but not limited to security managers and special security officers) whose duties involve managing or processing personnel security actions relating to the DoD PSP.

sensitive position. Any position so designated by the head of any department or DoD Component in accordance with E.O. 10450.

SON. A number that identifies the office that initiates the investigation and is recorded in the appropriate 'Agency Use' block of the investigative form. The SON is issued by OPM after authorization by the Office of the DDI(I&S).

SPēD. The SPēD Program is part of the DoD initiative to professionalize the security workforce. This initiative is intended to ensure that there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

SF 86. The standard form that the DoD uses for most national security background investigations. The automated version of the SF 86 is the e-QIP. As used in this manual, includes SF 86C and related forms.

supporting counterintelligence organization. The MDCO, as defined in DoDD 5240.06, supports CI issues involving military and civilian personnel. CI issues involving contractor personnel are referred to the FBI.

unfavorable national security determination. A denial or revocation of eligibility for access to classified information and or to occupy a sensitive position.

valid passport. A passport that is current (i.e., has not expired and has not been cancelled or revoked).

waiver. See "exception."

REFERENCES

Deputy Secretary of Defense Memorandum, "Defense Security Service (DSS) Future Options Study Recommendations," January 15, 2009[1]

Deputy Secretary of Defense Memorandum, "DoD Central Adjudications Facilities (CAF) Consolidation," October 20, 2010[1]

Deputy Under Secretary of Defense for Counterintelligence and Security Memorandum, "Personnel Security Issues," January 8, 2004[1]

Deputy Under Secretary of Defense for Intelligence and Security Memorandum, "DoD Security Lexicon," June 13, 2013

Director of National Intelligence Memorandum ES 2014-00674, "Adherence to Federal Laws Prohibiting Marijuana Use," October 25, 2014[1]

Director of National Intelligence Memorandum, "Delegation of Authority for the Director of Administration and Management to Determine Sensitive Compartmented Information Eligibility at the Department of Defense Consolidated Central Adjudication Facility," October 22, 2012[1]

DoD 3305.13-M, "DoD Security Accreditation and Certification," March 14, 2011, as amended

DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD 7000.14-R, "Department of Defense Financial Management Regulation: Accounting Policy and Procedures," current edition

DoD Directive 3700.01, "DoD Command and Control (C2) Enabling Capabilities," October 22, 2014, as amended

DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)," February 27, 2006

DoD Directive 5105.42, "Defense Security Service (DSS)" August 3, 2010, as amended

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended

DoD Directive 5210.48, "Credibility Assessment (CA) Program," April 24, 2015, as amended

DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

[1] Available from the Security Policy and Oversight Division, Office of the Director for Defense Intelligence, Intelligence and Security

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Instruction 3305.13, "DoD Security Education, Training, and Certification" February 13, 2014, as amended

DoD Instruction 5145.03, "Oversight of the DoD Personnel Security Programs," January 10, 2013, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program," March 21, 2014, as amended

DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Research, Development, Test, and Evaluation (RDT&E)", May 28, 2015, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011, as amended

DoD Instruction 5210.45, "Personnel Security Policies and Procedures for Sensitive Cryptologic Information in the National Security Agency/Central Security Service," November 14, 2008, as amended

DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010, as amended

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended

DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended

DoD Instruction 5505.07, "Titling and Indexing in Criminal Investigations," February 28, 2018

DoD Instruction 5505.16, "Investigations by DoD Components," June 23, 2017

DoD Instruction 6490.08, "Command Notification Requirements to Dispell Stigma in Providing Mental Health Care to Service Members," August 17, 2011

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction O-2000.16, Volume1, "DoD Antiterrorism (AT) Program Implementation: DoD AT Standards," November 17, 2016, as amended

DoD Manual 5105.21, Volume 3, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities," October 19, 2012, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5220.22, Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018, as amended

DoD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014, as amended

DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953, as amended

Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960

Executive Order 12564, "Drug-free Federal Workplace," September 15, 1986

Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended

Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended

Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008

Executive Order 13526, "Classified National Security Information," December 29, 2009

Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," August 18, 2010

Federal Acquisition Regulation, current edition

Federal Investigative Standards, December 14, 2012

Intelligence Community Directive 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008

Intelligence Community Policy Guidance number 704.1, "Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008

Intelligence Community Policy Guidance number 704.2, "Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008

Intelligence Community Policy Guidance number 704.3, "Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes," October 2, 2008

Intelligence Community Policy Guidance number 704.4, "Reciprocity of Personnel Security Clearance and Access Determinations," October 2, 2008

Intelligence Community Policy Guidance number 704.5, "Intelligence Community Personnel Security Database Scattered Castles," October 2, 2008

Memorandum of Agreement Among Defense Security Service, Defense Human Resources Activity's Defense Manpower Data Center, Deputy Under Secretary of Defense (HUMINT, Counterintelligence, and Security) and Deputy Under Secretary of Defense (Program Integration), February 2, 2010[1]

Office of Management and Budget Memorandum M-06-21, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006[2]

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005[2]

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," November 14, 2007[2]

Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence Memorandum, "Personal Attestations Upon the Granting of Security Access," February 9, 1999[1]

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of the Director of National Intelligence and the U.S. Office of Personnel, Management, "Approval of the Federal Investigative Standards," December 13, 2008[3]

Presidential Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Program, November 21, 2012

Presidential Policy Directive/PPD-19, "Protecting Whistleblowers with Access to Classified Information," October 10, 2012

Principal Deputy Under Secretary of Defense for Intelligence and the Administrative Assistant to the Secretary of the Air Force, "Memorandum of Agreement Concerning Transfer of Department of Defense Personnel Security Investigation Billing Function From the Defense Security Service to the Department of the Air Force," August 6, 2009[1]

Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019

The White House Memorandum, "Adjudicative Guidelines," December 29, 2005

U.S. Office of Personnel Management Booklet, "Requesting OPM Personnel Investigations," (also known as "INV 15")[4]

U.S. Office of Personnel Management Federal Investigations Notice Number 97-02, "Executive Order 12968 and Investigative Standards for Background Investigations for Access to Classified Information," July 29, 1997[5]

U.S. Office of Personnel Management Federal Investigative notice No. 05-04, "Reinvestigation Products for Positions Requiring Q, Top Secret or SCI Access," September 16, 2005

Under Secretary of Defense for Intelligence Memorandum, "Adjudicating Incomplete Personnel Security Investigations," March 10, 2010[1]

---

[2] Available at http://www.ncix.gov/SEA/reciprocity/policy.php
[3] Available to authorized users at https://www.intelink.gov/sites/jrt/Shared%20Documents/Federal%20Investigative%20Standards%20Final.pdf
[4] Available at http://222.opm.gov/investigations/background-investigations/reference/inv-15-requesting-opm-personnel-investigations/
[5] Available at http://www.opm.gov/investigate/archive/1997/fin9702.asp

Under Secretary of Defense for Intelligence Memorandum, "Authority to Suspend Contractor Personnel Security Clearances," May 13, 2009[1]

Under Secretary of Defense for Intelligence Memorandum, "Compartmented Program Collaboration, Reciprocity, and Oversight," August 9, 2011[1]

Under Secretary of Defense for Intelligence Memorandum, "Designation of the DoD Case Management and Adjudication Systems," April 10, 2009[1]

Under Secretary of Defense for Intelligence Memorandum, "DoD Personnel Security Adjudicator Professional Certification Program," January 28, 2014[1]

Under Secretary of Defense for Intelligence Memorandum, "Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," August 30, 2006[1]

Under Secretary of Defense for Intelligence Memorandum, "Implementation of the Rapid Assessment of Incomplete Security Evaluations (RAISE)," July 13, 2010[1]

Under Secretary of Defense for Intelligence Memorandum, "Personnel Security Clearance Adjudication Documentation," November 8, 2009[1]

Under Secretary of Defense for Intelligence Memorandum, "Review of the Adjudication Documentation, Accuracy and Rationales (RADAR) Assessments," August 31, 2010[1]

Under Secretary of Defense for Intelligence Memorandum, "Special Access Program Nomination Process," May 20, 2013[1]

Under Secretary of Defense for Personnel and Readiness Memorandum, "Implementation of the Position Designation Automated Tool," May 10, 2011[1]

United States Code, Title 5

United States Code, Title 18

United States Code. Title 21

United States Code. Title 50